特集 3

自己情報をどうコントロールするか
－SNS やアプリの利用を中心に －

原田 由里　Harada Yuri　**一般社団法人 EC ネットワーク理事**
安心して利用できる E コマース市場をめざして活動。ネット関連の消費者相談を受ける。
講演、啓発教材・書籍への寄稿や、関係省庁研究会、業界団体等委員会などに参加。

はじめに

ネット上の閲覧履歴や検索ワードなどが広告に利用されていることをご存じの人も多いと思います。特にサービスの多くを無料で利用できる SNS やアプリは、利用者側の情報を取得し、それをさまざまなビジネスに利用しています。

ただ、どの情報が取得されて、どのようなルートで利用されるのか確認し、きちんと内容を覚えている人は少ないのではないでしょうか。

身近で発生するネットトラブルには、利用者側がこうしたことに無関心であることが原因の１つであるものも少なくありません。今回は、よくあるトラブル事例から考えていきたいと思います。

ターゲティング広告がきっかけになったトラブル事例

・有名人が出ている広告の化粧品がお試し価格で購入できると思って申し込んだら、自動的に定期購入となった。
・以前から興味があったグリーンカード（アメリカ永住権）を申請できると思い、表示された広告を見たら海外の代理業者だった。

ターゲティング広告とは、利用者の検索履歴や閲覧履歴などを参考に、特定のサイトを訪れたときに、その利用者に合わせた広告が出される手法です。例えば SNS を利用する場合、その SNS に登録した自分の情報を利用して、その属性に合わせたターゲティング広告が表示されます。事例のケースでは、サイトの閲覧履歴から、日頃、興味のある広告が表示され、クリックしたことがトラブルのきっかけとなっています。

SNS の多くは広告収入により賄われていますので、広告表示を避けることはできませんが、広告は、年齢や性別、国籍などの属性に合わせて表示されていることを十分認識しておきましょう。男性には女性向けの広告は表示されませんし、海外の事業者の広告を表示することも可能です。ただ、広告の質まで個別審査されているとは限りませんので、見る側で注意が必要です。

ターゲティング広告への対策としては、サイトごとにオプトアウト（無効化）できる方法が記載されていますので確認してみてください。

いずれも個人情報が直接利用されているわけではありませんが、自分の情報がどのように広告に利用されるのか、これを機にアプリやサービスの利用規約やプライバシーポリシーなどで確認しておくとよいでしょう。

連携アプリがきっかけになったトラブル事例

・SNS に知り合いの名前で「サングラスが安い」という投稿が載っていたので、投稿文内の URL をクリックして商品を購入したが偽物だった。知り合いに尋ねると、自分は投稿していないという。
・SNS に「ポイントプレゼント」という

投稿があったので、URL をクリックしポイントサイトに登録したが、肝心のポイントは後から抽選だと知った。その後、自分の名前で同じ内容の投稿がされていることを知った。

連携アプリとは、外部のサービスやアプリと機能上のつながりを持つアプリのことです。アカウント情報（ユーザー名、パスワード）を入力しなくても外部のサービスが利用できるしくみですが、悪質な連携アプリがあるので注意が必要です。

SNS を利用していると、勧誘や広告サイトに誘導するようなメッセージが投稿されることがあります。この時、投稿文に貼られた URL をクリックすると、別サイトが立ち上がり、連携アプリへの許可を求められることがあります。「連携アプリを許可する」に同意すると、連携先のサービスに、SNS の登録情報の権限を渡すことになります（**図 1**）。

例えばメッセージの権限を許可すると、自分の SNS アカウント名で、連携先が勝手にメッセージを投稿することができます。

詐欺サイトに SNS のアカウントが乗っ取られる（実際に行われているのは「許可情報の委譲」）と、SNS でつながっている人に詐欺サイトへ誘導する投稿が流れ、その人たちが誘導先の URL をクリックし連携アプリを許可することで、さらに SNS でつながっている人へと連鎖的に流れていきます。

事例のケースも、SNS 上の知り合いの投稿だから安心と思ってクリックしたところ、悪意あるサービスのサイトに誘導され、そのサービスと連携してしまっていました。さらに、自分では何もしていないのに、SNS 上で勝手に投稿されていた事例もみられます。

Facebook 上では同様の手法により、「自己診断アプリ」の提供先が取得した Facebook 利用者の情報を、不正に流用していたという問題が発覚しました。流用は約 8700 万人分ともいわれています。

SNS 利用時は、連携アプリに簡単に権限を許可しないようにし、過去に許可した連携アプリがあれば、定期的に見直して連携解除することが必要です。

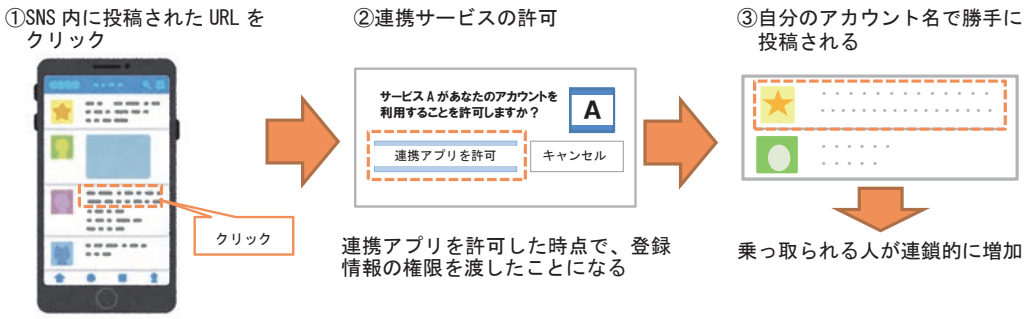
「○○がもらえる」「性格占い」などを楽しむ前に、連携アプリの許可を求められたら、ちょっと冷静になる必要があります。

不正アプリがきっかけになったトラブル事例

- SNS で知り合った異性から勧められたアプリを入れたらアドレス帳の情報が抜き取られ、過去に送った恥ずかしい写真を知人にばらまくと言われた。
- スマホに配送業者から不在通知の SMS が届いたので URL をクリックしたら、アプリがダウンロードされた。その後、勝手にアドレス帳登録者に同じ内容の文を SMS で配信され、さらに後日、キャリア決済で電子マネーが大量に購入されていたことが分かった。

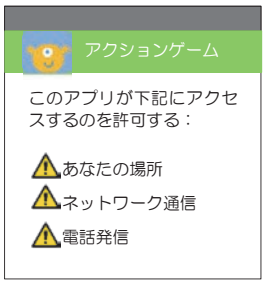
スマホには、電話番号や連絡先、位置情報や各アプリの履歴などの情報、また、メールや SMS（電話番号

図 1　連携アプリによるトラブル事例のイメージ



に送るショートメッセージ）の送受信、カメラやマイクなどの機能が付いています。アプリは、これらの情報や機能を利用することにより便利なサービスを提供することができます。

図２ アクセス許可の表示画面例



しかしアプリの中には、提供するサービスとは無関係の情報を取得するものもあります。アプリのサービス内容からみて不要と思えるような、たくさんの権限を与える必要はありません。

例えば Android の場合「アクセス許可」の画面で、アプリに権限を許可する項目が表示されますので、その内容を必ず確認しましょう（**図２**）。

また、Google Play などの正規アプリストア以外から入れる「野良アプリ」は危険です。例えば、リンク先から直接ダウンロードして野良アプリを入れようとすると「提供元不明のアプリ」と表示されます。それを許可し、さらにアクセス許可を求める画面も、その内容を確認せずに許可して入れてしまうと、許可した情報や機能が相手に渡り、悪用される危険があります。

各情報へのアクセス権や SMS の送受信機能などが悪用されると、アドレス帳登録者に SMS を送りつけて被害を拡大させることがあります。また、キャリア決済（携帯電話料金合算払い）するのに必要な情報が漏えいすると、前述のトラブル事例のような、なりすましによる金銭被害が発生することもあります。

いずれにしても、アプリに与える権限によっては、スマホが乗っ取られた状態になり得ることがあります。

子どもの見守りアプリなども、使い方によってはストーカーに悪用される可能性があります。他人にスマホは触らせず、定期的に持っているアプリの見直しをしてください。

不正確な登録情報が原因のトラブル事例

- アダルトの広告が嫌で未成年で登録していたが機能制限があるので不便。登録年齢を変更したいができない。
- 不正ログインの被害にあい、本人確認のためアドレスと生年月日を聞かれたが、登録情報を思い出せない。

SNS やアプリなどに登録する際、その情報が、広告を含め色々利用されているということは分かりました。すると、こう考える人がいます。「個人情報の悪用や漏えいに備えて、最初から虚偽の個人情報で登録しておこう」と。

これは決してお勧めしません。不正ログインやパスワード失念などで本人確認が必要な際に思い出せなかったり、身分証明書を要求された際に情報が一致しなかったりする可能性があるからです。本名や年齢が自由に変更できると犯罪に悪用されることから、その回数等を制限していることもあります。

SNS やアプリでは、利用規約などで登録情報の正確性や情報管理を利用者側に課しています。正しくない情報で不利益を被っても、誰も助けられません。個人情報を相手に渡すのが不安であれば、初めから利用しない、登録しないというのも選択肢に入れてください。

おわりに

自分が渡した情報を後から回収したり、渡した先の情報漏えいや悪用を利用者側から防いだりすることはできませんが、渡す情報を、ある程度自分でコントロールすることはできます。

少なくとも、何も考えず、何も読まずに、簡単に「許可」「同意」「登録」することが危険だということは、ご理解いただけたのではないかと思います。SNS やアプリの利用には、常に情報管理意識が求められているのです。