平成 28 年度ネットトラブル注意報

- 第１号「スマートフォンを持つ上で気をつけたいこと」（平成２８年４月）
- 第２号「スマートフォンを持つ上で気をつけたいこと　その２」（平成２８年５月）
- 第３号「外出先の無線ＬＡＮ接続による危険性と対策」（平成２８年６月）
- 第４号「インターネット上における拡散行為の危険性」（平成２８年７月）
- 第５号「ネットゲームによるトラブルについて」（平成２８年８月）
- 第６号「著作権侵害について知っておきたいこと」（平成２８年９月）
- 第７号「友人間で起こるコミュニケーションアプリでのトラブル」（平成２８年１０月）
- 第８号「SNS を利用する際に気を付けること」（平成２８年１１月）
- 第９号「インターネットでの個人間取引で気を付けたいこと」（平成２８年１２月）
- 第１０号「なりすましや不正アクセスによる被害と対策について」（平成２９年１月）
- 第１１号「ネット上の迷惑行為への対策について」（平成２９年２月）
- 第１２号「新学期に向けて注意をしてほしいこと」（平成２９年３月）

◆◆◆平成２８年度第１号「スマートフォンを持つ上で気をつけたいこと」◆◆◆

■スマートフォンの普及とネットトラブルの増加

携帯電話やスマートフォンが急速に普及し、私たちの生活はより便利に、より快適なものになりました。今ではスマートフォンが主流になってきています。では、具体的にどれほど普及しているのでしょうか？

内閣府調査によれば、平成２３年の高校生のスマートフォン所有・利用率は６.８％、携帯電話は８８.８％だったのに対し、平成２７年はスマートフォン所有・利用率は９３.６％、携帯電話は３.９％となっています。つまり、この４年間でスマートフォンのシェアが大幅に拡大し、普及したということになります。

警察庁は、インターネットを通じて１８歳未満の児童生徒が犯罪に遭遇しないよう、平成２５年１０月から全国の警察で「サイバー補導」を導入しました。平成２６年には４３９人、平成２７年には５３３人（９４人増）の１８歳未満の少年らが補導されています。補導された少年らの平均年齢は１６．５歳で、最年少は１２歳の中学１年生男女２人、年齢別で最も多かったのは１７歳の２３６人です。そのうち７１．８％は非行・補導歴がなく、更に１８、１９歳も含めた補導人数は６６６人にも上ります。

年々スマートフォンの利用者は低年齢化してきています。「うちの子に限って･･･」という意識ではなく、ネットトラブルは誰にでも起こり得るという姿勢が望ましいと言えるでしょう。

【無料通話アプリやＳＮＳなどによるいじめ】

無料通話アプリでは、メッセージのやり取りを、同じグループ内でしか読むことができないため、特定の人を仲間はずれにしてグループを作ったり、招待して即退会させるなど、いじめの手段として使用されるケースがあります。

また、メッセージを読むと「既読」というマークが付き、メッセージを読んだことが分かる仕組みになっています。このことから、メッセージを読んでも返信しない場合は「無視された」と捉えられ、いじめに発展するケースもあります。

さらに、ネット上で「死ね」「殺す」等のメッセージを送られたことで、不登校になったり、命に係わる事件が起きたりしています。

【見知らぬ人との出会いによるトラブル】

女子中学生がチャットやメールで知り合った男性から、自分の裸の画像を送るよう強要され、男性が逮捕される事件が起こっています。

ネットでのトラブルに巻き込まれないためには、ＳＮＳ上で安易に個人情報を伝えないなどの注意をする必要があります。

また、無料通話アプリのロゴを真似たマークを使い登録を促し、出会い系サイトに誘導する事件も報告されています。手口が巧妙化しており、自分では気が付かないうちに出会い系サイトに登録されることもあります。

■トラブルの対策

【フィルタリングサービスを利用する】

携帯電話会社等が提供するフィルタリングサービスに加入すると、子供の年齢に応じて、有害なサイトへアクセスを防ぐことができます。

（※フィルタリングをかけても閲覧できる有害サイトもあり、注意が必要です。）

【ネットの安全な利用方法を考える】

ＳＮＳにあるプロフィールや写真が、実際のものであるかどうかを見抜くことは大変困難です。「良い人を装った悪い人」とネットで知り合い信用した結果、個人情報や写真、無料通話アプリなどのＩＤを交換したり、直接会いに行ったりしたために犯罪被害を受けるケースが増加しています。

子供たちに、ネットを利用することが危険と隣り合わせであることを認識させるとともに、ネットの安全な利用方法について、子供たち自身が考えるよう促すことが大切です。

◆◆◆平成２８年度第２号「スマートフォンを持つ上で気をつけたいこと　その２」◆◆◆

スマートフォンには便利な機能がたくさんあります。中でも、自分の現在地が確認できる GPS 機能や、ボタンひとつでゲームや音楽プレイヤーとして使えるアプリなどは、お使いの方も多いのではないでしょうか。いずれの機能も自分で簡単に設定でき、スマートフォンをより便利で有益なものにすることができます。一方で、安易な判断で取り入れてしまうと、思わぬトラブルを引き起こすこともあります。今回は、スマートフォンを持つ上で気を付けたい２つの点についてお伝えします。

■GPS 機能による位置情報発信による被害

GPS（Global Positioning System）とは、人工衛星を利用して、自分が地球上のどこにいるのかを正確に割り出すシステムです。この GPS 機能を設定したスマートフォンを所持していれば、自分の現在地を確認することができます。特に保護者の方には、子どもの居場所を確認するために利用したい機能かもしれません。

さらには、どこかへ出かけるとき、現在地から目的地までの移動時間はもちろん、移動ルートも知ることができ、迷わず容易に目的地にたどり着くことができます。

実はこの GPS 機能、自覚がないまま設定していることが多く、そのために思わぬトラブルを引き起こすことがあるのです。

例えば、位置情報の設定を ON にしている状態で、自宅や学校などで写真を撮り、SNS サイトに投稿し

た場合、その投稿や写真自体に撮影場所が記録されてしまいます。それらの投稿や写真から簡単に自宅や学校の所在地が分かってしまい、実際にストーカーや誘拐などの被害にあう事件も起きています。
まずは自分のスマートフォンの設定を確認し、位置情報の利用について正しく認識した上で各種機能を活用する必要があります。

■不正アプリのインストールによる個人情報の漏えい

スマートフォンにインストールすることで、活用できるソフトウェアをアプリと呼びます。さまざまな目的のもとに作られるアプリは年々増加しています。
日常的に使用できるものや娯楽性の高いもの、有料や無料のものなど、数多くありますが、中にはスマートフォン内の個人情報を盗むウイルスが仕込まれている不正なアプリも存在しています。そのようなアプリをインストールしてしまうと、個人情報が漏えいし、自分自身はもちろん、電話帳に登録している知人にまで被害が及ぶこともあるのです。このような思わぬ事態を招かぬよう、自分がインストールしようとしているアプリが安全なものかどうか、判別するポイントを紹介します。
アプリをインストールする際、端末の中にある連絡先等へのアクセス権限を求められることがありますが、不要な権限を求めるアプリには注意が必要です。そのアプリの機能や性質、目的を考え、本当に必要な権限の許可を求めているかどうかを考えることが大切です。もちろん、電話帳データなど個人情報へのアクセスを求めるアプリの全てが不正なものとは限りませが、そのアプリに対するユーザーレビューやコメント、開発会社の評判やソフトウェアの更新頻度なども確認しながら、信頼できるアプリかどうかを判断してください。合わせて、スマートフォンにセキュリティソフトをダウンロードし、アプリを取り入れる際に安全性をチェックすることも大切です。少しの工夫で、不正アプリのインストールを避けることが可能になりますので、日頃から心がけておきましょう。

◆◆◆平成２８年度第３号「外出先の無線ＬＡＮ接続による危険性と対策」◆◆◆

無線 LAN とは、無線でネットワークに接続する通信システムのことです。街中では、無料で無線ＬＡＮに接続できるアクセスポイントも多くあり、簡単にインターネットに接続することが可能なため、利用する機会も多いと思いますが、接続することによりトラブルが生じることもあります。そこで、今回は外出先で無線 LAN に接続することの危険性とその対策についてお伝えします。

■個人情報の窃取

公衆無線 LAN スポット（Wi-Fi スポット）は、携帯会社を選ばず、有料契約の必要もないため、外出先でも気軽にインターネットに接続することができます。場所によっては、スマートフォンの回線よりも快適に利用することができ、写真などのアップロードも早く、大容量のダウンロードも可能です。通信制限もかからないので、外出時にはとても便利です。
しかし、公衆無線 LAN スポットは、通信が暗号化されていないものもあり、メールの内容を盗み見されたり、スマートフォンに保存していた連絡先や写真、動画などの個人情報が盗み取られてしまう危険性があります。
インターネット上で情報を暗号化して送受信できる仕組みを SSL（Secure Sockets Layer の略）と言います。これは、個人情報、クレジットカード情報などの大切なデータを安全にやりとりするためのシステムで、SSL が運用されているかどうかは、URL が https://で始まっていること、ブラウザに鍵マークが表示されていることで確認できます。公衆無線 LAN スポットを利用する際は、この暗号化処理がされているかどうか確認することが重要です。また、利用しない場合は Wi-Fi の設定をあらかじめ切っておくと安心でしょう。

■情報の傍受

無線 LAN に接続する際、通常はパスワードの入力が必要になります。これは、無線 LAN 通信時に、第三者からの盗聴や盗難等を防ぐために暗号化の仕組みが使用されているためです。しかし、公衆無線 LAN スポットには暗号化されておらずパスワードを要求しないものもあります。そのような公衆無線 LAN スポットに接続してしまった場合、結果として自分のスマートフォンに他人がアクセスし、乗っ取られてしまい、知らぬ間にマイクやカメラを勝手に操作され盗聴や盗撮に使われたり、サイトにログインする際の ID やパスワードを盗み取られてしまう危険性があります。

公衆無線ＬＡＮに接続する際は、パスワード等を要求しないアクセスポイントは避けることが必要です。また、そのような公衆無線ＬＡＮスポットをやむをえず利用する場合でも、個人 ID やパスワードでのログインが必要なサイトは閲覧しないことが大切です。

クレジットカード情報を盗まれたり、ウイルスファイルが自動でダウンロードされたりと、悪意のあるサイトも存在すると言われていますが、誰でも接続できるアクセスポイントを利用することで、そのようなサイトに接続してしまう危険性も高まります。誰が提供しているスポットかを確認し、提供元が不明確なものは極力接続しないようにしましょう。

＜対策のポイント＞

・通信が暗号化処理されているかの確認をする
・公衆無線 LAN スポットを利用しない時は Wi-Fi 設定を切る
・パスワードのないアクセスポイントは利用しない
・ログインに ID やパスワードが必要なサイトは公衆無線ＬＡＮ使用時には閲覧しない
・誰が提供しているか不明なアクセスポイントには極力接続しない

◆◆◆平成２８年度第４号「インターネット上における拡散行為の危険性不適切な投稿について」◆◆◆

インターネットでは、掲示板やブログやＳＮＳによって、一度に多くの人に情報を発信することができ、情報を受け取った人がそれをさらに多くの人に伝えることで、短期間に情報が拡散していきます。これは、多くの人に情報を伝えたいときには、大変便利な機能ですが、使い方を誤ると危険なこともあります。今回は、このような拡散行為が招くトラブルと対策についてお伝えします。

■誤った情報が広がってしまう

大震災の際、インターネットを利用することで、被災地の現状や必要な物資を全国に伝えられ、適切な支援に繋げることができました。しかし、一部で誤った情報や虚偽の情報が流され、それを信じた人が、心配してさらに情報を拡散したことで、被災地に不要な物資がたくさん届き、それを処理するために貴重な人手と多額の費用が必要となり、被災地に迷惑をかけることがありました。

インターネット上の情報は、「いつ、どこで、誰が」発信した情報なのかを確かめ、信頼できる情報なのかを見極めることが大切です。

■拡散行為の危険性

ＳＮＳでは、他の人の書き込みをそのままの形で紹介する機能があります。面白い書き込みや気になる書き込みを見つけたとき、簡単に友達などに紹介することができるので、利用している人も多いのではないでしょうか。

しかし、この行為は、罪に問われる可能性があり注意が必要です。
例えば、「○○が××で逮捕された」という情報をその情報の真偽に関わらず、自分のＳＮＳサイトで紹介した場合、名誉棄損罪等に問われる可能性があります。
知人や友達からの情報だからといって、それが必ずしも事実とは限りません。また、他人の名誉や犯罪に関する情報については、拡散すべきではありません。本当にその投稿は拡散してよい内容なのか、拡散した場合にどのような影響があるのかについて、よく考えることが大切です。

■ネット上にあげる前に確認すること
これから夏季休業に入ると家族や友人との旅行などの記録や思い出の写真等を、ネット上に掲載する機会が増えるかもしれません。その際、その情報によって他人が不快に感じる可能性はないか、写真に写っている人はネット上に掲載することを承諾しているのか等について確認することが必要です。ネット上にあげた情報は拡散される危険性があります。一度、ネット上にあげた情報を完全に削除することは難しいため、安易にネット上にあげないことを心がけるとともに、送信する前に十分確認することが大切です。

◆◆◆平成２８年度第５号「ネットゲームによるトラブルについて」◆◆◆

家庭用ゲーム機やパソコンだけでなく、携帯電話やスマートフォンで、いつでも、どこでもネットゲームを楽しむことが出来るようになりました。外出先や移動中にネットゲームをすることによるトラブルや、ゲームを長時間するようになってしまうなどの影響がでています。
みなさんの中にも、ネットゲームに熱中するあまり、夜遅くまで遊んでしまう人や、歩きスマホをしていて危ない思いをした人がいるかもしれません。
今回は、ネットゲームにおけるトラブルについて紹介します。この話を参考にして、ネットゲームとの正しい付き合い方について考えてもらいたいと思います。

■「歩きスマホ」や「～ながらスマホ」の危険性
先般、位置情報を活用したスマートフォンゲームが配信され、日本各地で「～ながらスマホ」による事故の発生が報告されています。ゲームをしながらの「歩きスマホ」や自転車や自動車運転中の「～ながらスマホ」による交通事故はもちろん、路上でのひったくり被害や不審者被害も報告されています。また、深夜にゲームをしながら街を歩くことで、深夜徘徊で児童生徒が補導されるといったことも発生しています。

■公共の場での利用に注意
スマートフォンを人に向けてゲームをしてしまい、盗撮を疑われたり、進入禁止の場所でゲームをしたりするなどのトラブルが報告されています。電車内等の公共の場では、周りの状況をよく確認し、他人に迷惑をかける恐れがないか確認する必要があります。マナーを守った利用を行ってください。

■課金トラブル
ネットゲームには、ゲーム内で使用するアイテムを購入できるものがあります。支払の方法は、クレジットカードやプリペイドカードによるものなどがあります。クレジットカードや電話料金合算払いは、後の請求となるため、気づかないうちに請求が高額となる可能性があります。アイテムを購入する場合には、保護者に事前に相談するなど、トラブルを避けるための事前のルールづくりが大切です。

■ネットゲームのトラブル

ネットゲームの中にはアイテムを交換したり、プレイヤー同士が会話したりすることができるものがあります。アイテム交換を持ち掛けられ、結果として詐欺等の被害にあうケースがあります。ゲーム内で知りあう人の中には、悪意を持って接触してくる人もいます。安易にメールアドレスや電話番号などの個人情報を相手に伝えることは避ける必要があります。

■ネットゲームはネット依存の入り口

ゲームを有利に進めようとすると、つい長時間プレイしてしまいます。また、ゲームによっては利用者が午後 11 時から午前 2 時頃に最も多く、利用する時間が深夜になるものもあります。ゲームに熱中するあまり睡眠不足や昼夜逆転の生活になることやゲームで知り合った人物とのトラブルで実生活に悪影響があってはいけません。

ゲームを含むネットの利用について、使用する時間や場所を家族で話し合い、ルールを決めて、そのルールを守ることが大切です。

◆◆◆平成２８年度第６号「著作権侵害について知っておきたいこと」◆◆◆

インターネットが利用できる機器は、パソコンだけでなくスマートフォンにまで拡大し、SNS 等による情報発信の機会が増えました。好きな音楽や面白い動画を SNS に投稿することが習慣になっている人もいます。しかし、雑誌の記事やテレビ番組、ＣＤやＤＶＤの音楽や映像には、著作権があります。今回は、気づかないうちに著作権を侵害してしまわないように、注意すべきポイントについてお伝えします。

■著作権侵害に該当する行為について

漫画、音楽作品、映画などには、その作品を作った人に著作権があります。これを著作者に無断でコピーし、ネット上に投稿したり、友達に送信したりすることは、著作権侵害にあたります。

例えば、好きな芸能人の画像や漫画のキャラクターのイラストを、SNS のプロフィール画像として使用したり、カラオケ店でのカラオケの音源や映像そのものを、ネット上に投稿したりする行為も著作権侵害にあたる可能性があります。

■著作権侵害は犯罪です

無断で漫画雑誌の誌面を写真撮影してネット上の動画サイトに投稿し、不特定多数に閲覧させた疑いで中学生が逮捕された事件がありました。

また、漫画、CD、DVD などの映像や音源をコピーしてサイト上に投稿するだけでなく、映像や音源が違法にネット上に投稿されているものと知りながら、ダウンロードすることも著作権侵害になるので絶対にやめましょう。

■気を付けたいポイント

スマートフォンのアプリケーション（以下アプリ）の中には、無料で音楽をダウンロードできると紹介されているものがあります。しかし、これらは違法に音楽をダウンロードするアプリの可能性があります。

サービスを提供しているアプリに「JASRAC 許諾番号」が記載されているか（日本の音楽の著作権を管理している団体「JASRAC」の許可を得ているか）を確認すると良いでしょう。

携帯電話やスマートフォンが高性能化し、録音や録画が簡単にできるようになりましたが、自分が録音、録画したものをネット上に投稿する前に、著作権の侵害になるかどうかを確認する習慣を是非身に付けてください。

◆◆◆平成２８年度第７号「友人間で起こるコミュニケーションアプリでのトラブル」◆◆◆

友人と連絡を取る方法として近年増えているのが、スマートフォンなどのモバイル端末で使用されるコミュニケーションアプリです。メールが手紙だとしたら、コミュニケーションアプリは会話に近いリアルタイム性を持ったコミュニケーション手段です。

手軽で便利というメリットから多くの人が利用していますが、文字だけでは真意が伝わりにくく、それがトラブルに発展するというデメリットもあります。今回は、コミュニケーションアプリでトラブルにならないための注意点をお伝えします。

■言葉の解釈の違いによるトラブル

友人と遊ぶ約束をしていたＡさんは、コミュニケーションアプリを通して「何で来るの？」と当日の交通手段を聞きました。すると突然友人から「遊べなくなった」と返信がきました。後日、友人のＳＮＳには自分と遊ぶ約束をしていた日に、違う人と遊びに行った投稿が掲載されました。それをきっかけに、二人は会話もしなくなり、お互いを避けるようになりました。何が原因だったのでしょう？

それは「何で来るの？」という返信を友人は「なぜ来るの？」という意味で受け取ってしまったからです。コミュニケーションアプリでは、普段の会話のようについ思ったままを送ってしまいがちですが、文字は様々な解釈を生み、それがトラブルの原因になることがあります。一部のコミュニケーションアプリでは、発言が取り消せないものもあるため、正しい内容が伝わるように、日頃から相手がどう受け取るか考え、文章を読み返すなどしてメッセージを送るように心がけることが大切です。

■メッセージを送る時間帯

友人と寝る時間を削って深夜までコミュニケーションアプリでメッセージのやり取りを毎日続けていたＢさんは、常に寝不足状態で学校の成績にも影響が出てしまい、次第に体調を崩すようになりました。

深夜のメッセージは、眠りを妨げられ寝不足になるだけでなく、グループで会話をしている場合は通知が鳴りやまないなど、相手に迷惑をかけてしまう場合があります。人によって生活のリズムも違うので、翌日でも支障がない内容ならば、深夜にメッセージを送らないようにしましょう。また、深夜にメッセージが送られてくることが気になるようならば、通知を切っておくことも大切です。

■メッセージの終わらせ方

友人とコミュニケーションアプリでメッセージのやり取りをしていたＣさんは、友人との会話が楽しく、長時間に渡りやり取りを続けていました。暇な時間があればとにかく誰かにメッセージを送信し、他愛もない会話を続けるといったことを毎日していたところ、次第にメッセージを返してくれる友人が減っていき、学校でもぎくしゃくした関係になってしまいました。

長時間に渡るメッセージのやり取りは、自分は楽しくても相手が同じように思っているかはわかりません。メッセージが続くと、終わりにするタイミングを見失ってしまうことがあるかもしれません。会話の途中で「時間は大丈夫？」など気遣うメッセージを間に挟むことで、話を切り上げるタイミングを相手に作ることができます。また、会話を終わらせたい場合、「今日はありがとう」「話せてうれしかった」などと伝え、話の終わりを感じさせることも有効です。相手の気持ちを考えた利用を心がけましょう。

◆◆◆平成２８年度第８号「SNS を利用する際に気を付けること」◆◆◆

SNS は、インターネットを通して友だち同士の交流を深めるコミュニケーションツールとして大変便利なものです。個人で撮影した写真や動画を SNS 上に投稿する人が増えてきていますが、今回は、SNS を利用する際に気を付けたいことについてお伝えします。

■個人情報の流出

スマートフォンでは、GPS 機能を利用した位置情報サービスを利用することができ、目的地への交通手段などを調べるときなどに大変便利ですが、その GPS 機能を「オン」にしたまま写真を撮り、SNS などに投稿した場合、写真を撮った場所をネット上に公開してしまうことになります。

実際に、自宅で撮った画像に位置情報が付いていて、知らないうちに住所を他人に知られていたというトラブルが発生しています。必要のない時には、カメラの GPS 機能を「オフ」にしておくことが大切です。

■アカウントの乗っ取り

芸能人の使用する SNS が不正にログインされるという事件も起こっていますが、パスワードの設定、管理の甘さが原因のようです。

SNS のアカウントを他人に乗っ取られると、自分の投稿が削除され、全く身に覚えのない投稿が行われてしまうだけでなく、SNS で繋がっている人に、悪質な広告メールが送られるなど、他人にも迷惑をかける恐れがあります。

乗っ取られたことに気が付いたときは、すぐにパスワードを変更してください。また、すでにパスワードが変更されてしまった場合は、ログインすることもできないので、すぐに、その SNS の公式サイト等で、乗っ取られた場合の対応を確認の上、適切に対応して、二次被害を防ぐことが大切です。

また、SNS のアカウントを乗っ取られる経験をした人の多くは、ネット上の色々なサービスで、同じアカウントとパスワードを使っていることがあるようです。乗っ取ろうとする人は、セキュリティの甘いネットサービスから利用者情報（アカウントやパスワード）を抜き取り、その情報で、ラインやフェイスブックなど他のサービスにログインできるか、手当たりしだいに試しているようです。

したがって、乗っ取りの防止策として、パスワードを使いまわさないことが大切です。パスワードを全く違うものにするのが難しい場合には、同じパスワード部分にサービスに応じて自分のルールで文字を追加したり、定期的にパスワードを変更して、その変更日時をパスワードに追加したりするなど、工夫することが大切です。

◆◆◆平成２８年度第９号「インターネットでの個人間取引で気を付けたいこと」◆◆◆

インターネット上での個人間取引と言えばオークションサービスを連想する人も多いと思いますが、スマートフォンの普及により最近ではフリーマーケットサービスを提供するフリマアプリ（商品を売買する場を提供するサービス）が人気を集めています。

しかし、未成年者は、原則、保護者の同意を得なければ、売買をすることができません。

多くのフリマアプリの利用規約には、未成年者が利用する場合は保護者の同意を得ることと書かれています。フリマアプリを使って、保護者に相談せずに一人で商品やお金のやりとりをすることは避けましょう。

また、保護者の同意を得た上でフリマアプリを利用する場合にも、トラブルが発生する可能性がありますので、今回紹介するトラブルの具体例や対処法を理解した上で利用しましょう。

■購入時のトラブル

フリマアプリを利用する人の中には、中古品を新品だと偽ったり、偽物のブランド品を出品したりする人もいます。取引相手の情報をプロフィールや取引実績などで確認することが大切です。また、フリマアプリでは数枚の商品写真と商品説明のみでは判断がしづらいため、ほしい商品が出品されていても、特に高価なものは安易に購入することは避けた方が良いでしょう。

購入した商品がネットの説明に記載されていたものと異なる状態の場合、返金を求めることができます。その場合には取引完了に必要な「受け取り評価」をしないようにしましょう。受け取り評価をしなければ、運営側が預かっている代金が出品者に支払われることはありません。

■送料のトラブル

送料負担が購入者側なのか出品者側なのか、商品説明にあらかじめ記載されていますが見落としがちです。送料込みと記載されているのに着払いで届いたというトラブルも頻発しています。事前にどちらが負担するのか確認するよう心がけましょう。

明記されたものと違う場合は、まず受け取り拒否をしてそのまま商品を送り返し、出品者に元払いで再発送してもらうようメッセージを送ると良いでしょう。

■その他、気を付けたいこと

出品者の評価や、過去の出品履歴を見て、事前にトラブルを回避することが重要ですが、それでもトラブルに発展することもあります。多くのフリマアプリ運営会社の規約では、商品等でトラブルが起きた場合は、当事者間で解決すると定められています。何かがあれば自己責任であることを認識した上で、利用規約をしっかり読み、サービス内容を理解して利用することが大切です。また、当事者同士で解決できない場合には、消費生活支援センターに相談しましょう。

◆◆◆平成２８年度第１０号「なりすましや不正アクセスによる被害と対策について」◆◆◆

名前やプロフィールを特定の人に似せてアカウントを作成し、その人になりすましてメッセージを送信したり、書き込みをしたりする「ＳＮＳでのなりすまし」が増加しています。なりすましに気が付かずにやり取りをしているうちに、有料サイトに誘導されてしまうなど被害が出ています。

また、不正アクセスによるアカウントの乗っ取りも増加しています。アカウントを乗っ取られると、個人情報の漏えいや金銭的被害を招くこともあります。

今回は、なりすましや不正アクセスによる被害の実例とその対策についてお伝えします。

■なりすましによる被害と対策

日頃からＳＮＳを利用して、友人と交流を行っていたＡさんは、ある日、友人から「いつもとは違うアカウントからメッセージが送られてきたけど、もうひとつアカウントを作ったの？」と聞かれました。Ａさんは、ひとつのアカウントしか持っておらず、身に覚えがなかったため、不審に思い調べたところ、誰かがＡさんの名前や写真を勝手に使用してＡさんになりすましている別のアカウントを見つけました。そのアカウントを使って、他人の悪口や卑猥な書き込みを行っていたため、Ａさんはすぐにサービス提供会社に連絡をとりました。そのアカウントがなりすまされたものであることが証明されたため、アカウントは凍結され、その後Ａさんは友人にも状況を理解してもらい、被害を最小限に留めることができました。

このように、なりすましは自分より他の誰かが気がついて発覚することが多くあります。もし、友人から普段とは違うアカウントを使った様子の違うメッセージが届いた場合、本当にその友人かどうかを確認すること、直接本人に連絡してみることはお互いの身を守る上でとても大事なことです。自分はもちろん、大切な友人が被害に巻き込まれないよう、できることから始めてみましょう。

■不正アクセスによる被害と対策

不正アクセスとは、他者のＩＤやパスワードを入力するなどして、本人にしか利用できない機能を他者が利用できる状態にすることです。不正アクセスされると、その後にＩＤやパスワードが変更され、本人が利用できない状態にされたり、本人になりすまされて様々な不正を行われたりすることになります。

ＩＤやパスワードを盗み取る手口としては、普段利用しているサイトを装った全く別のサイトに誘導してＩＤやパスワードを入力させるケースや、ウイルスを仕掛けてＩＤやパスワードを盗むケースなどがあり、とても巧妙です。

不正なアクセスをされた場合、インターネットショッピングなどで不正に商品を購入されたりする可能性があります。また、ＳＮＳで繋がっている人に対して、電子マネーの購入を要求したり、不正アプリのダウンロードを促すなど、家族や友人が被害にあうこともあります。

不正アクセスを防ぐためには、パスワードの設定を工夫することが大切です。生年月日など推測されやすいパスワードは避け、例えば**「ａ」を「@」**に、**「ｌ（小文字のエル）」を「１（数字のイチ）」**にするなど簡単な工夫をするだけで安全性が高まります。複数のサービスで、同じＩＤ・パスワードは使用しない、パスワードは定期的に変更するなどで、自ら被害に遭わないよう、心掛けるようにしましょう。

なお、不正アクセスは「犯罪行為」です。もしも被害にあった場合は、サービス提供会社への通報とともに、警察に被害届を出して相談しましょう。

◆◆◆平成２８年度第１１号「ネット上の迷惑行為への対策について」◆◆◆

みなさんの中には、迷惑メールを受信したり、出会い系サイトに誘導するような書き込みをＳＮＳ上でされたりした人がいるかもしれません。最近では、このような迷惑行為はとても巧妙になっており、知らないうちに自分だけでなく、友人にまで被害が及ぶ可能性があります。安心してSNSを楽しむために、今回はネット上の迷惑行為への対策についてお伝えします。

■自分が迷惑行為の加害側になってしまう危険性について

SNSの投稿の中には、詐欺サイトへ誘導するリンクが含まれるものや、個人情報を盗むための不正アプリをインストールさせようとするものがあります。知らない人からの投稿であれば、警戒して被害に遭わない場合も多いのですが、知り合いから来た場合は、被害にあう危険性が高まります。

こんな事例があります。ＡさんがＳＮＳを利用中、面白い動画の投稿を見つけて、その動画を友人とシェア（共有）しました。友人は「Ａさんがシェアしているものだから大丈夫」と思い、その動画の再生ボタンを押したところ、ウイルスに感染させるためのサイトに誘導され、結果としてスマートフォンから個人情報が盗まれ、SNSアカウントが乗っ取られてしまうというものでした。

他にも、「無料動画を見るためにアプリをインストールする必要がある」と画面表示され、不正なアプリをインストールするよう誘導する手口もあります。インストールしてしまうと、アプリが自身のSNSアカウントとの連携を許可し、友人に対してアダルトサイトに誘導したり、金銭を要求したりする内容の投稿などをしてしまいます。このように、自分でも気が付かないうちに迷惑行為の加害側になってしまう場合もあります。

■ネット上の迷惑行為への対策

自分が迷惑行為の加害者にならないためには、たとえ友人の投稿でも、怪しい動画やURLは安易にクリックしないようにしましょう。自分では身に覚えのない投稿がＳＮＳ上でされている場合は、不正アプリがインストールされ、自分のアカウントが乗っ取られている可能性があります。まず設定画面から、不審なアプリがインストールされていないか確認を行い、インストールされている場合は速やかに削除するなどの対応を取りましょう。

「〇〇診断」などのタイトルのついたアプリの中には、不正なものも含まれている可能性があるので、インストールしたり、個人情報を入力したりする場合は十分に注意しましょう。また、友人から不審な内容の投稿が繰り返されている場合は、本人に直接確認するようにしましょう。さらに、スマートフォンでもウイルス感染の可能性はありますので、信頼できるセキュリティソフトを入れるなどの対策も有効です。

◆◆◆平成２８年度第１２号「画像の無断掲載による危険性について」◆◆◆

新学期を控えたこの時期に、子供にスマートフォンを買い与える御家庭も多いのではないのでしょうか。卒業式や入学式の記念に写真を撮影し、その様子をSNSで友達と共有しようとする人が増えるのもこの時期です。今回は、そんな時期に注意して欲しいことについてお伝えします。

■入学前にネット上で友達を作る危険性

最近では、同じ学校に入学する予定の児童生徒で、入学前からネット上で友達を作ろうとする人がいます。例えば、SNSのプロフィールに「〇〇学校入学予定」などと書き込み、入学前からネット上でつながろうとしたりします。前もってつながりを作ることで安心感を得られる一方、トラブルが生じる可能性もあります。ネット上でのやり取りが原因で喧嘩となってしまうケース、SNSグループの参加人数が多くなり、通知が鳴りやまず、睡眠時間を削られてしまうケースなどがあります。また、同じ学校の入学予定者だと思っていた相手が、実際には出会い系や個人情報を入手する目的で偽っている人物である可能性もあります。入学前にネット上で友達を作る危険性について十分理解し、不審な点や危険な点があれば保護者や教員へ相談することが必要です。

■卒業式、入学式等に際して

卒業式や入学式の記念に、撮影した写真をSNSに掲載する児童生徒は多いと思いますが、SNS上に掲載すると制服等から学校名が分かってしまう可能性があります。また、写真は誰でも保存可能なため、悪用される危険性があります。許可を取らずに友達と一緒に写っている写真を掲載すると、友達ともトラブルになる可能性があります。他にも、卒業後にクラスの生徒と連絡がとれるように、クラス全体のSNS上のグループを作るなど、この時期はネット上でつながっている友達が多くなる傾向があります。SNSに掲載した情報は不特定多数の人物が閲覧する可能性があることをしっかり理解し、自身及び友達の写真や、進学先等については掲載することの危険性をしっかりと認識しましょう。

■保護者に注意してほしいこと

情報社会が進む中で、今後ますますスマートフォンの所有者は低年齢化が進むと考えられます。お子様用のスマートフォンの購入にあたっては、必要性や危険性を総合的に判断していただくことが大切です。情報の取捨選択ができない段階では、閲覧できるサイトをフィルタリングで制限するなどの対策が必要です。また、フィルタリングをかけて終わりではなく、フィルタリングの内容やスマートフォンの設定等について、保護者が子供と一緒に定期的に見直しをすることがトラブル防止の有効な方法です。

正しい使い方をすればスマートフォンはとても便利なツールです。未来を担う子供たちを守るために、大人が協力して見守っていきましょう。