(スライド1)

(自己紹介・あいさつ)

まずは記念に写真を撮りたいと思います。

(GPSをオンにしたまま写真を撮影し、ツールとともにデータ配布する)

今日は皆さんにITリテラシーについていくつかお話しさせていただくわけですが、既に授業でも学ばれていることがあると思います。今回は実際に起こった事件などを題材に、こういったトラブルから身を守るための対策などをお話しできればと思います。

また、これまで学んできたITリテラシーについても、より深く考えてもらえればと思います。よろしくお願いします。

本日は主に以下の3点について、お話しさせていただきます。

(スライド2)

SNSの恐怖、スマホアプリに潜む問題、便利アプリの落とし穴と題してお話ししたいと思います。

(スライド3)

それではさっそく、SNSの恐怖から。

(スライド4)

皆さん方はスマートフォンを使っている人が大多数と聞いていますので、こういったアイコンに見覚えのある方は多いかと思います。

(スライド5)

各アイコンはそれぞれ、Twitter、Google+、LINE、FaceBookを指していますが、これらは共通して一つのジャンル名としても呼ばれています。

(スライド6)

SNS、ソーシャルネットワークサービスといいますが、これは親しい人同士がコミュニケーションを取るために便利なシステム、とでも考えてもらえればいいかと思います。お互いの近況を話し合ったり、メッセージを送ったりと、とても便利なツールですが、最近これらのツールで、特に若年層を中心にいろいろなトラブルが起こるようになってきました。それが・・・

(スライド7)

通称、炎上と呼ばれる事件です。炎上とは、不謹慎な発言や行動を公開してしまうことにより、いっせいにネット上・現実世界で叩かれるといった事態を指しますが、この原因は何なのかという点について考えてみたいと思います。

(スライド8)

これは主にTwitterでの炎上事件をまとめたページですが、このようなまとめが作られるほど、炎上事件というのは多発しているわけですね。では、このようなトラブルに巻き込まれると最悪どうなるのか。

(スライド9)

SNSは匿名でやっているから、などと考えているかもしれませんが、過去の炎上事件でも、同様に匿名であった人の個人情報はかなりの確率で暴かれています。

(スライド10)

その後に始まるのは、関係各所へ電話・メール・FAX、時には郵便も含めた、通報という名の攻撃が始まります。炎上の規模にもよりますが、おそらくこういった学校レベルの回線ならすぐにパンクして、学校の業務に大きな支障が出るでしょう。

運がよければ数日程度で鎮火しますが、場合によっては年単位で攻撃が続くこともあります。

そしてその後には・・・

(スライド11)

というような運命が待ち受けているわけですね。

大げさだと思うかもしれませんが、炎上のきっかけとなった内容によっては、逮捕や拘留は十分あり得ます。先日もしまむらでの土下座事件で北海道の主婦が逮捕されていましたね。

もちろんそんな事態になっては、学校側も自主退学を進めたり、もしくは強制的に退学にすることもあるでしょう。逮捕されなくても、迷惑行為が原因で退学になったという事例は、大学での話ですがありましたし、高校でも当然あり得る話ですね。

仕事をしている人なら解雇もあります。大体逮捕されたら、仮に冤罪であったとしても解雇というのが日本企業のスタイルですので、よほどの大企業や公務員など、一部の例外以外は逮捕されれば仕事を失います。また逮捕されなくても、電凸やメールなどの攻撃が続いて業務にならないとなれば、原因となった社員をクビにして沈静化を図る、というのはある種当然ですね。

また、これは自分だけに限った話ではありません。恋人がいたならその恋人の勤務先、両親がいるならご両親の勤務先、場合によっては親族まで巻き込んで攻撃が続くことがあります。そうなると恋人も最悪クビになり、ご両親もクビになり、といった形で巻き込まれ、一家離散という事にもなりかねません。

そして、この時代一度ネットで拡散した情報は消すことができません。自分の名前で検索すると、過去に犯した犯罪や炎上事件がずっと表示され続けるわけです。海外では「忘れられる権利」として、そういった過去の情報を消せるような、表示させなくするようなシステムやルールを作れないか、という話も持ち上がっていますが、なかなかこれも難しいでしょう。

さて、炎上事件を起こすとどうなるか、という話をしたところで、ではどのように個人情報が暴かれるのか、という話をしておきましょう。

(スライド12)

まずはプロフィールとか居住地を確認します。これだけで大体絞り込める場合もありますが、ニックネームからでも名前の推測ができます。海外は分かりやすくて、例えばレベッカという名前ならニックネームは大体ベッキーになりますが、日本でも本名に紐付いているニックネーム、例えばヒロと呼ばれているなら、ひろゆき、ひろし、ひろかず、といったように、ある程度の法則を元に推測が可能ですね。

さらに過去の発言や、ターゲットと会話をしている他のユーザーとの発言を摺り合わせるなどすれば、確実に市レベルくらいまでなら絞り込むことが可能です。例えば電車通勤・通学をしているなら、電車待ってる、とか駅に着いた、なんて発言の時間を調べることで、特に電車の本数の少ない田舎なら、どの駅で乗り降りしているかという事まで掴めます。駅までの移動手段も、徒歩なのか自転車なのか、あるいは送り迎えしてもらっているのか、という事が分かれば、最寄り駅からどの程度の圏内に住んでいるのか、ということも分かりますね。

発言やプロフィールを精査することでそのくらいまでは掴めますが、さらに確実性を増すのが写真です。例えば、行きつけの本屋です、という写真をアップしたとします。その写真をもとに、Google類似画像検索にかけます。そして、その本屋さんのWebサイトが出てきたらどうでしょうか。本屋さんの住所が分かるわけですね。本屋さんの住所が分かれば、行きつけというくらいなのだから近距離、さらに高校生ならば片道5キロ程度の圏内だろう、という推測ができます。ここで住所がさらに絞り込まれていくわけですね。

この頃になると、協力者がその近辺の写真を撮影したり、犯人らしき人間をリストアップし、卒業アルバムのデータ等を提供するなどして犯人の絞り込みに協力したりします。そのようなターゲットに近い人物からの協力もあわせれば、ほぼ確実に個人情報は暴かれてしまうでしょう。

さて、最後の写真一枚でカタが付く、という話ですが、ここで授業の最初に始めたデータ転送も終わったようなので、

(スライド13)

ワークショップということで、皆さんに少し手を動かしていただきたいと思います。

(スライド14)

デスクトップにあるexif-toolというフォルダを開いて、Exif読取り君.exeという実行ファイルをダブルクリックしてください。

そうするとプログラムが立ち上がりますので、

(スライド15)

ファイル・開くから、gazou.jpgというファイルを開いてください。そうすると、いろいろなデータが出てくると思うんですが、そのいろいろなデータが出ている、画面下半分辺りで右クリックをして、そのメニューの中から地図上に位置表示を選んで、クリックしてみてください。

(スライド16)

こんな感じのメニューが出ればOKです。地図上に位置表示を選んでみてください。

・・・(確認してもらう時間)

みなさんに確認してもらった通り、何も考えずにスマートフォンのカメラアプリを使っていると、GPS情報が付いてしまい、意図しないところで個人情報が漏れることがあると分かったかと思います。他にもカメラの種類など、いろいろなデータが、このEXIFという情報には含まれるわけですね。

Twitter自身が運営している画像アップロードサービスや、たいていのサービスではこのようなEXIF情報は消去されることが多いのですが、一部のサービスやブログなどでは消去されないままになることがあります。

自宅の住所や居場所を特定される可能性もありますので、GPSデータは記録されないように設定しておきましょう。

(スライド17)

まずAndroidの場合から説明します。ただし、Androidは端末ごとにアプリの設定方法が大きく異なっているので、あくまで一例ということで、シャープ製の端末・SH-02Eの純正カメラアプリを元に説明します。他の機種のカメラアプリも似たような操作でできると思いますので、詳しくは各機種のマニュアルを参考にしてみてください。

(スライド18)

カメラアプリを立ち上げたら、設定をタップして、保存設定をタップします。次の画面に出る自動位置情報付加メニューをタップします。

(スライド19)

Offをタップします。これで位置情報機能がオフになります。

(スライド20)

また、GPS情報を使うアプリを開始した場合に、このような画面が出ることがあります。GPS情報を記録したくない場合には、必ず同意しないを選びましょう。ただし全てのアプリでこのような通知が出るわけではないので、注意しておいてください。

(スライド21)

iPhoneの設定についても説明しましょう。こちらは端末を作っているメーカーがAppleだけということもあって、Androidよりも分かりやすいです。

(スライド22)

歯車の形をした設定アイコンをタップすると、この左のような画面になるので、プライバシーという項目を探します。プライバシーをタップすると右のような画面になるので、位置情報サービスというメニューをタップしてください。

(スライド23)

位置情報メニューからGPSを許可する、しないという設定ができるので、ここからカメラのGPS設定をオフにします。

iPhoneの場合、どのアプリもここからGPS設定ができるので、位置情報を利用しているアプリが分からなくて困ったら、ここから設定しましょう。

(スライド24)

では、SNSでの炎上や、個人情報漏洩編被害を防ぐためにはどうすればいいかを説明します。

1つめですが、当たり前のことではありますが、違法行為や俺ってこんなに悪いんだぜ、といった悪事の自慢をしないこと。炎上の大半が、この種の発言をした人に対して起こっています。

2つめ、こちらも当たり前ですが、他人に対してひどい言葉を吐かないこと。自分は普通に話しているつもりでも、口頭で話している言葉と、文字だけの言葉では、受け取る人や場合によって大きく印象が違ってきます。自分は冗談のつもりでも、相手はその言葉にひどく腹が立ったり、恨まれたりすることもあります。そうすると、本来なら炎上しないような発言から炎上する、ということも起こりうるわけですね。

3つめ、これは先の2つと違って防衛的な話になりますが、個人情報を特定されそうな情報は極力載せないということです。例えば電車に乗って、しばらく時間をずらしてから電車に乗ったよーと投稿するとか、ダミーの情報を入れておくというのも有効です。

最後に、Twitterをはじめとした SNSは、気軽に書き込め、ついつい身内の人間しか見ていない気持ちになりますが、全世界に公開されているものです。大通りに立って、大声で叫んでいるようなものなのです。気軽に書いた内容を公開する前に、この内容は公開しても大丈夫かどうか、深呼吸して考えるくらいがちょうど良いかもしれませんね。

(スライド25)

さて、主にTwitterや開かれたSNSの話をしてきましたが、最後に、全く触れていなかったLINEについてお話ししましょう。ひみつ、と題していますが、知っている人は知っていることなので、面白味はないかもしれません。

(スライド26)

LINEのトーク内容は運営側で読むことができます。当たり前と思われるかもしれませんが、普通のメールなどと違って一対一で送っているわけではなく、LINEが運営しているサーバーを経由して通信しているので、技術的な話として、内容はチェックできます。

また、LINEでは迷惑行為を行うユーザーを通報するという機能がありますが、その場合、過去のトーク内容100発言が運営に送られ、チェックされます。

(スライド27)

去年の12月くらいからそのような機能が追加されていることが分かります。また、利用規約でも、内容はチェックすることがあるよ、とちゃんと書かれていますので、内容は筒抜けと考えてもいいでしょう。

誰にも読めないと考えて傍若無人に振る舞っていると、内容によっては逮捕や補導といった事に発展することがあります。また、運営している人がいい人とかどうかも分かりません。情報漏洩事件では、内部の人間による犯行が最も多いというデータもあります。勝手にトーク内容を盗み見て、それを元に脅迫されたり、住所を知られてストーキングされるなどといった恐れもあります。

時間の都合でLINEのみ取り上げましたが、他のツールでも同様に運営者側でのチェックをうたっているツール、うたっていないけれどもチェックが可能であるツールもあります。公にしてはまずい内容は、こういったツールで話さない方がいいでしょう。

(スライド28)

ここからは、スマホアプリが抱える問題について、お話ししていきたいと思います。この問題は、主にAndroidを使っている人に気をつけてもらいたい内容です。iPhoneももちろん気をつけなければいけないのですが、特にAndroid環境で問題が起こっています。

(スライド29)

特に有名な事件がこれです。the movie事件とも呼ばれていますが、例えば桃太郎電鉄 the movieといった、正式なアプリ名・Androidでは出ていないアプリ名のあとに、the movieという言葉を入れ、本物と間違えてダウンロードする人を狙ったスパイアプリでした。

このアプリを入れると、ゲームの動画などが流れるのですが、その裏で電話帳のデータを抜き取り、外部のサーバーに送っていたんですね。このようなアプリは他にもありまして、

(スライド30)

このような記事も出ています。例としては、メモリクリーナーと名乗っているけれど何もせず、その裏で電話帳やメールアドレス・Webのアクセス履歴などを送信したりするソフトがありました。他にも電波状況をよくするとか、バッテリーを節約する、ウイルス対策というソフトに見せかけた例が報告されています。

Androidは、基本審査なしに公式のマーケットに誰でもアプリを掲載することができるため、こういったセキュリティの問題が起こりやすくなっています。いまは自動でマーケットに提供されたアプリをチェックし、問題があれば公開されなくなるプログラムが動いていますが、それをすり抜けるものもあるので完璧とはいえません。

(スライド31)

そういったニセアプリに騙されないためには、この4点に気をつけるようにしましょう。

Androidではアンチウイルス、ウイルス対策ソフトがありますので、それを入れておきましょう。とはいえ、これはAndroidの仕様上、気休め程度の効果しかないと思っておいた方がいいので、これに頼りきりではいけません。このウイルス対策ソフトにも偽物があったりしますので、例えばdocomoならdocomo自身が純正のウイルス対策ソフトを出していますのでそれを利用する、他社のウイルス対策ソフトを利用する場合は、パソコンで有名なウイルス対策ソフトメーカーの製品を使うといいでしょう。無料で利用できるものも多くあります。

2つめ。導入しようと思うアプリの評判は必ず確認しましょう。レビューだけではなく、ネットでそのアプリ名で検索してみて、マイナスの評価が多くないか確認しましょう。ただ、登場したばかりのアプリやマイナーなアプリだと、この方法はなかなか難しいかもしれません。

そういったときに重要なのが、インストール時に出てくるアプリの利用権限です。

(スライド32)

この画面はあるアルバムソフトをインストールするときに出てきた画面ですが、これはそんなにあやしいとは言えませんね。

(スライド33)

では例えば、ただの画像アルバムソフトに、こんな権限が求められたらどうでしょうか。メッセージの内容や電話帳の内容の閲覧や通話履歴などのデータにまでアクセスするアプリとなっています。これはちょっとあやしいな、ということになりますね。

もちろん権限をたくさん求めるからスパイアプリだ、とは言い切れませんが、こういうアプリの内容に対して求めてくる権限が多すぎたり、これは要らないだろうというところまで権限を求めてくるアプリには、注意しておいた方がいいでしょう。

(スライド34)

では最後の4点目です。いくら慣れていても、自分ではなかなかどのアプリがスパイアプリなのか見分けが付かないということもあると思います。そういう時は、他の人に頼りましょう。

Androidマーケットには審査がありませんが、そのアプリをダウンロードしてレビューし、アプリ自体の性能はもとより、あやしい動作をしないか、まともに使えるかということをチェックしてくれているサイトがあります。

(スライド35)

有名なサイトはこちら、アンドロイダーというサイトです。アプリ開発者の方や経験を積んだ方、著名なユーザーがアプリの動作チェックを行っているので、ここでレビューされているアプリはおおむね問題がないと言えるでしょう。

(スライド36)

さて、ここまでiPhoneには全く触れていませんでしたが、iPhoneの場合だと、インストール時にはAndroidのように権限の確認画面は出ませんが、設定画面から一括で全てのアプリの各権限の許可・拒否ができます。

(スライド37)

また、アプリを起動したときに、初めてその機能にアクセスしようとしたときは、このように確認画面が出ます。この例ではカレンダー機能にアクセスしようとしていますが、これが嫌なら許可しないを選べば、そのアプリはその機能にアクセスできません。

Androidでは、インストールするときに権限を確認してインストールしたら、そのアプリには許可した機能が全て許可されてしまいますが、iPhoneだとその都度警告が出たり、一括で特定の機能へのアクセスだけオフにできますので、比較的セキュリティに配慮されているのかな、と思います。

(スライド38)

ということで、この4点に注意してアプリのダウンロードや利用を行ってください。また、主にAndroidの話ばかりでしたが、iPhoneでも過去に似たようなアプリはありました。

また余談ですが、LINE等の一部ソフトは電話帳を運営者のサーバーに対してアップロードしています。それによって友人同士をマッチングして、友達リストに名前が出てくるんですが、暗号化されているとはいうものの、その電話帳のデータがこれからもきちんと管理されるのか、自分だけならまだしも友人や知り合いのデータをアップロードすることで、その人に迷惑はかからないか、運営者のサーバーが攻撃されてデータを盗まれないかなど、自分の知らないところで情報漏洩が起こる可能性は年々高まっています。

アプリの仕組みを理解することで、そういったトラブルの可能性を減らすことができますので、アプリは注意してインストール・使用するようにしましょう。

(スライド39)

では最後のトピック、位置情報アプリの危険性についてです。写真に含まれるGPS情報で住所などがバレるかも、という話は先にしましたが、ここではより積極的に位置情報を利用したアプリを使う場合の危険性についてお話しします。

(スライド40)

ここで取り上げるのは、Foursquareというアプリです。聞き覚えが無い人もいるかもしれませんが、世界的にも有名な位置情報を利用したアプリで、位置情報SNSとして広まっています。

他には、日本産のアプリですとイマココ、というアプリがあります。これはiPhoneにしかまだないようですが、主な機能はFoursquareとよく似ています。これらのアプリを使う上での注意点などを説明します。

(スライド41)

その前に、このアプリの機能を説明しましょう。主な機能としては、自分が今いる場所をアプリから通知して、同じアプリを使っている人やFoursquareに会員登録している人と共有することができます。

また、その位置情報の通知をチェックインといいますが、その回数によってポイントが貯まったり、オリジナルのバッジマークが利用できるようになったりと、ある種ゲームのようにランクアップできるのが特徴です。

これだけなら、せいぜい同じFoursquareの会員だけに通知されるということで、そこまで大きな問題にはなりにくそうですが、まあ既にFoursquareの会員数も世界で2000万人を超えているようですから、それでもなかなか脅威な訳ですけども・・・

(スライド42)

このように、TwitterやFacebookにもチェックイン通知を流せるわけですね。例えば意図せず投稿をしてしまったがために、自宅の情報、通っている学校名などがバレてしまう、ということがあるわけです。先に述べた炎上事件では、このような情報も発掘され、最大限に活用されますので、一つのミスが命取りになる可能性があります。

ただ、これらは常にチェックインがTwitterに流れるわけではなく、自分以外にはチェックイン情報を公開しない設定もありますので、適切に設定さえしておけば、そこまで恐れることはありません。

ここで一番恐れるべき事は、

(スライド43)

ここが田舎だということです。

都会であれば、ある場所に今いるよーとチェックインしたとしても、大多数の人に紛れたり、単なる通りすがりであったりもするため、そこまで個人の特定はできません。ですがこの市内で、例えばセブンなう、とかつぶやいてチェックインすると、時間帯によっては客が自分しかいない、ということもあるわけですね。

想像して欲しいのですが、例えばあなたがストーカーに狙われているとしましょう。そしてあなたはそれに気づいていないとします。そのストーカーは、ネットでのあなたの発言が気にくわなくて、密かにあなたの居所や行動パターンを調べようと考えています。

そんな時、このようなチェックインを不用意にしてしまうと、場合によってはそのストーカーに顔まで知られてしまうことになるわけですね。

(スライド44)

まとめです。位置情報アプリは利用するシチュエーションに注意し、必要なとき以外は利用しないこと。また、利用する場合は設定などをよく確認して、個人情報が不用意に漏れないように気をつけることですね。

また、皆さんが住んでいるこの周辺は田舎であることをよく認識してもらって、個人の特定は都会での利用者より容易であることに注意しておいてください。

余談ですが、知り合いの人はこのアプリで、閉店前の某薬局からチェックインしてTwitterで全体公開していました。その薬局は僕もよく行くんですが、閉店前なんて多くても2・3人しかお客さんはいないんですよね。これ、ほぼ確実に特定できるなーと思ったことがあります。

もちろん都会でも油断は禁物ではありますが、ネットの世界では都会でも田舎でも同じようにサービスが受けられるとはいっても、地域によってアプリの使い勝手・使い方の注意点は変わります。どうしてもアプリは東京などの大都市圏で開発されることが多く、かつユーザーも大都市に住んでいる方が相対的に多いです。そしてそういった最新のアプリをチェックして、こういった使い方があるよ、とブログ等でレビューするのも大都市圏のユーザーが多いわけです。

そうすると、都会では便利で楽しく使えるアプリやサービスでも、それを田舎で使う場合には、マイナスの影響が出たり、もしくは全く使えないという事もありうるわけですね。アプリを利用するということ一つ取っても、大都市と地方ではまた違った心構えが必要になることもある、ということをよく覚えておいてください。

(スライド45)

それでは今日のまとめです。

ひとつめ、ネットでは内輪のノリというものは通用しません。投稿した内容は、世界中の人が見ています。Twitterの投稿内容はYahooのリアルタイム検索を使えば検索もできます。友達以外にも、たくさんの人が発言をチェックしているという気持ちを持っておいてください。

ふたつめ。臆病者とはいい響きではありませんが、それくらいの気持ちで危険から避けるように行動しないと、ふとしたことから個人情報が暴かれる事態ともなりかねません。これくらいなら大丈夫だろうという油断が、あとで大きな被害をもたらすこともあるのです。

最後に、これは臆病であれという話と近いものがありますが、私の好きな言葉の一つです。発言した人が誰かというのは諸説ありますが、この言葉は危機管理におけるキャッチフレーズとして、今でも広く使い続けられています。

まずは炎上事件などを起こさないように、悲観的になって徹底的に気をつける。しかしもし起こってしまったときは、徹底的に準備をした内容に従い、きっと大丈夫だ、と楽観的に対応した方がミスなく問題を沈静化できる、という意味です。

皆さんも普段の行動はできる限り慎重に、臆病と言われるくらいに気をつけつつ、いざ問題が起こったときは、それまで慎重に行動した内容を踏まえて自信を持ち、気持ちを楽に持って対応するという行動を心がけるようにしてみてください。

以上、ご清聴ありがとうございました。

（以降、時間が余れば質疑応答）