（あいさつ・スライド表紙）

今日は皆さんに、ネットで発生したセキュリティ問題などについて、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かと思います。今年実際に起こった事件などを題材に、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。

さて、内容に入る前に、余談ではありますが、皆さんエゴサーチという言葉を知っていますか。Google等の検索エンジンで、自分の名前を検索して評判などを調べる行動をエゴサーチと言いますが、私の名前＋香川 なんてキーワードでエゴサーチすると、私のWebサイトより先に香川大学出身のお医者さんの名前が出てくるんですね。

年齢も私とそう変わらないようで、Facebookや他のサービスでも、私よりその方が知名度高いんですね。なので、例えば友達から自分の知らない友達を紹介されたときに、詳しいプロフィールは話さずに、ネットで検索してくれたらすぐ出てきますよ、等と言ってごまかすことがあるのですが、その方と次にお目にかかったときには、お医者さんなんですかーすごいですねーなんて言葉をいただくことが度々ありました。

私のWebサイトも順位は下の方ですが出てきますので、決して嘘は言っていませんよね。ですがその方は、私のことを医者だと思い込んでしまった。それは例えば、お医者さんの知り合いがいれば、何かあったときに助かるだろうという考えがあったから、そう信じ込んでしまったのかもしれません。

こういった心の働きは心理学(脳生理学)などでも知られているようで、こんな言葉があります。

（スライド1）

「人は自分が信じたいと思うものを信じる」。この言葉は、かのシーザーが「人間ならば誰にでも、現実のすべてが見えるわけではない。多くの人は、見たいと欲する現実しか見ていない」という、良く似た言葉を残しているくらいで、これを元にした言葉なのかもしれませんが、紀元前の頃から人の本質は変わっていないことが分かる言葉ですね。

まさに人が騙される際には、このようなバイアス、偏りや思い込みなどという意味ですが、それを利用されることが少なくありません。それを防ぐにはどうすればいいか、というようなことを考えながら、これから一時間お付き合いいただければと思います。

（講義内容スライド）

ということで、本日の講義内容はこのようになっております。ずっと私がしゃべりっぱなしというわけではなく、ところどころで皆さんの手を動かしていただく予定ですので、よろしくお願いします。

（講義内容スライド・LINE乗っ取り事件）

まずは大きな話題となったLINE乗っ取り事件について、LINE社から発表された内容や、識者の方の見解・推測などを踏まえて、この攻撃が利用されたのではないかなというお話をさせていただきます。

（LINEスライド1）

皆さん方の中には、こんなメッセージか来た方もいるかもしれません。突然LINEの友達から、今は自分が忙しいので、代わりにWebMoneyやiTunesカードを買ってきてほしいと依頼されるという、今年の夏前頃から秋口にかけて、かなり大規模に行われた攻撃でした。

LINE社が公表していないため総数は不明ですが、相当数のアカウントが乗っ取られ、このような詐欺に使われたと考えられています。そして、このアカウント乗っ取りに使われたと考えられている攻撃方法が……

（LINEスライド2）

パスワードリスト攻撃とよばれるものです。ここ最近、LINEだけではなく、多くのサイトがこの手法での攻撃を受けていると言われています。

（LINEスライド3）

パスワードリスト攻撃を図にしたものがこれです。まず、何らかの方法でIDとパスワードのリストを入手します。これには、様々な方法で攻撃して直接盗み出す方法や、他から盗まれた情報をアンダーグラウンドマーケットで購入するなど様々です。

その後、ターゲットとなる相手に、盗んだIDとパスワードをそのまま使ってログインできるかどうかを試す、という攻撃を行います。

LINEでいうと、LINEにはスマートフォンからではなく、PCからログインするという機能がありました。その機能を使う場合、スマートフォンからメールアドレスとパスワードを登録する必要があったのですが、そのパスワードに、他のサービスで使っていたものと同じものを使っていた人が乗っ取られた、ということになります。

まとめると、

(LINEスライド4)

こんな感じですね。では、対策はと言うと……

(LINEスライド5)

この2つがあげられます。2段階認証というのは、LINEの場合で言うと、PINコードという、4ケタの暗証番号のことです。PCで使うためのメールアドレスとパスワードとは別に、このPINコードを別途設定しておけば、仮にパスワードを使い回ししていても、このコードが分からなければログインできないため、多少は安全という理屈です。

余談ですが、当初このPINコードは必ず設定しておかないといけないわけではなく、任意でした。しかし乗っ取り多発後にこのPINコードの設定が必須となり、結果的に乗っ取り被害がほぼ終息したということです。このことから、効果的な防御手段の一つと言えるでしょう。

といっても、全てのサービスが2段階認証に対応しているわけではないですし、パスワードの使い回しをしないということが、セキュリティ対策の原則です。でも、パスワートを複数覚えるなんて面倒だし、という方もいるでしょう。そこで、参考までに私が行っている対策としては、

(LINEスライド6)

この2点となります。一番オススメなのはパスワード管理ソフトを使うこと。スマートフォンでもPCでも、パスワード管理ソフトはいろいろ出ています。それらを使ってパスワードを管理すれば、比較的安全にいろいろなサービスを利用することができるでしょう。

2点目の、特定のフレーズと数字の組み合わせについては、例を見ていただくと分かりやすいかと思いますが、abcとdefghiの間に数字を入れていますね。これを例えば、LINEなら01、Twitterなら02といったように、サービス毎に変えていくという方法です。

ひとつのフレーズと、各サービスごとの組み合わせだけ覚えていればいいので、私も頻繁に手で入力しないといけないWebサービスなどではこの手法を使っています。各サービスの組み合わせを覚えるのが面倒な場合は、01 LINE、02 Twitterのように、フレーズ自体は紙に書かず、この数字の組み合わせだけメモするようにすれば、仮にそのメモを他人に見られた場合にも多少は安心できると思います。

ということで、パスワードリスト攻撃の概要と対策を、LINE乗っ取り事件を例に説明しました。続いては……

(講義内容スライド・スマホアプリ逮捕事件)

スマホアプリでの逮捕事件について説明していきたいと思います。

(スマホアプリ・スライド1)

今年10月、このような事件がありました。スマートフォンで画像を簡単に共有できるというアプリが、この「写真カプセル」だけではなく、他にもいくつかありますが、まず、これらのアプリの仕組みについて説明します。

(スマホアプリ・スライド2)

この図の通りではありますが、アプリを使って、アプリ開発元が管理しているサーバーに画像データをアップロードします。それを同じアプリを使っているユーザーが、専用のキーワードを入力してダウンロードするという流れになっています。

ここで、そのキーワードを使ってデータをダウンロードする際に、対価としてアプリ内通貨を設定することができるんですね。その仕組みが次のスライドになります。

(スマホアプリ・スライド3)

写真カプセルの場合は「カギ」という名前ですが、これを1個100円で販売しています。1つのカギで、一つのキーワードのデータを閲覧できる仕組みです。データをダウンロードしたいユーザーは、このカギをアプリ開発元から購入します。

アップロードしたユーザーは画像にアクセスがある度に、ポイントを獲得します。これを貯めるとカギやAmazonギフト券などに交換できるため、お小遣い稼ぎとか、カギを購入せずにデータを見たいというユーザーがデータのアップロードをする、という循環になっているわけですね。

こういった、アクセスに応じて報酬が出るという仕組みで運営されているサービスに、例えばFC2動画などもありますが、あちらも法律に触れている内容のデータをアップロードした人が捕まっていたりしますね。

では、どうしてアップロードした人が分かるのか、という点についてですが、

(スマホアプリ・スライド4)

IPアドレスというものがあるからなんですね。こんな赤字で書くほどのものではありませんが、これについては皆さんも教科書などで知っているかもしれませんね。

IPアドレスは、よくインターネット上での住所です、とも言われますが、スマートフォンでもPCでも、このIPアドレスは必ず割り当てられています。割り当てるのはプロバイダーやキャリア、例えばドコモやau、OCNやYahoo! BBなどがそうですが、自分がインターネットに接続するときに利用している業者さんがIPアドレスをたくさん持っていて、使う度にユーザーに割り当てるという形になっているわけですね。

その割り当て表はキャリアやプロバイダが持っているので、警察から問い合わせがあると、そのデータを提供するため、本人が特定できるというわけですね。

こう言うと、警察以外の個人ではIPアドレスで身元特定はできないと思われがちですが、IPアドレスからある程度の住所を推定する方法というものもあります。それが……

(スマホアプリ・スライド5)

IP ジオロケーションと呼ばれる技術です。IPアドレスから位置情報を得る技術で、IPアドレスごとにデータベースを利用して、ざっくりとした位置情報を特定したり、スマートフォンなどではGPSと組み合わせて、より詳細な位置情報を得ることもできます。

では、そろそろ話を聞いているだけでは退屈になってきたかと思いますので、少し手を動かしていただきましょう。

(スマホアプリ・スライド6)

このアドレスにアクセスしてみてください。

・・・(確認してもらう時間)

ページは開いたでしょうか。

(スマホアプリ・スライド7)

無事に開きましたら、ページの左側にこんな表示がされていると思います。この教室からのアクセスだと具体的な場所は表示されないのですが、Network(ASN)に、KAGAWA-EDUと記載されていますね。少なくともこれで、香川県の教育機関からアクセスしているということは分かるわけです。

これを元に、例えば学校から他のWebサイトなどに攻撃を行ったりすると、被害を受けた側から香川県に問い合わせを行い、攻撃を行った当人を特定する、ということが可能なわけですね。

(スマホアプリ・スライド8)

例えばこれは、私の運営しているサーバーに対して攻撃を行っていると思われるデータですが、こういったアクセスログというものをどこのサービスでも取っています。

この攻撃してきた時間とIPアドレスを付き合わせてやれば、容易に本人の特定は可能です

から、インターネットは匿名で何をしても大丈夫な場所ではなく、法に触れる行為や不用意な言動・行動によって、それ相応の罰を受けるという、現実と変わらない空間なのだということを覚えておいてください。

続いては……

（講義内容スライド・セレブ画像流出事件）

この件についてお話ししていきましょう。

（セレブ画像流出・スライド1）

日本では海外ほど話題になっていなかった感もありますが、今年8月末から9月頭にかけて、ハリウッドの有名女優の撮影していた画像や動画が流出する事件がありました。このデータはiPhoneユーザーがデータを保存することができる、iCloudに不正アクセスされて流出したものとされています。

この攻撃には、先に述べたようなパスワードリスト攻撃や、「iPhoneを探す」機能に脆弱性が含まれていて、それを利用されたという説もありますが、そのほかに使われたと考えられる攻撃が

（セレブ画像流出・スライド2）

秘密の質問への攻撃ですね。この秘密の質問は、パスワードを忘れた場合に

（セレブ画像流出・スライド3）

こんな画面で秘密の質問に対する答えを入力すると、パスワードをリセットして、新しいパスワードを画面に表示してくれたり、メールで送ってくれるという形が一般的です。

皆さんは、こういった質問に対する答えに、正直な内容を入れていませんか？ 私たちのような一般人ならいざ知らず、セレブとしてテレビや映画にたくさん出演している人の個人情報は、本人が語ったり、取材の結果明らかになったりで、多くの人が知っているものがあります。

この例のように、ペットの好物などについても知られている可能性がありますし、生年月日は当然知られているでしょうから、簡単にパスワードがリセットされてしまう、という事に繋がるわけですね。

では、我々のような一般人はそんなの関係ないと思われるかもしれませんが、そうではありません。

（セレブ画像流出・スライド4）

このデータは平成25年の不正アクセス事件について、警察庁が発表している統計情報ですが、これを見ると被疑者は10代が最多であることが分かります。

下の表は犯行動機のデータになっていますが、オンラインゲームでの不正操作や嫌がらせ、好奇心を満たすためという理由が多く見られます。

これらの内容と、実際に起こった事件などをあわせて考えると、10代の被疑者は比較的金銭目的ではなく、個人的な恨みや好奇心を元に犯行を行っていると推測されます。その場合、ターゲットとなるのは、同じ年代の皆さん方の可能性が高いでしょう。例えば、ケンカしたりして仲が悪くなった友人に対して、なりすまし等の攻撃を行う、といった感じですね。

クラスメイトであれば、個人情報もある程度は分かりますし、自分が分からないことでも、他のクラスメイトや友人を通して知ることは簡単にできますね。そこで、秘密の質問に設定してある質問と答えがうまくマッチすれば、アカウントを乗っ取られる、ということにも繋がっていくのです。

（セレブ画像流出・スライド5）

そういう現実を踏まえて対策としては、秘密の質問に対する答えにフェイク、または全く関係ない内容を入れること。例えばペットの好物は、という質問に対し、単三電池と入れる等ですね。

質問が決め打ちで、自分で設定できない場合は、このように答えに嘘を入れるくらいしかありませんが、サービスによっては、質問の文章も自分で作れるサイトもあります。そう

いうところでは、質問にも推測不可能な内容、この例のように世界の真理を尋ねてみてもいいでしょう。

ついついこういった質問には、忘れないために正直な内容を記載しがちになりますが、あえて色々フェイクを入れることも、身を守るには必要だということを覚えていただければと思います。

(講義内容スライド・Webサイト調査)

続いては最近かなり数が増えている、危険なサイトについての話です。詐欺サイト、フィッシングサイト、ウイルスをばらまくサイトなど、危険なサイトはたくさんありますが、今回はそれらをひっくるめた調査方法について、お話ししたいと思います。

(Webサイト調査・スライド1)

Google Chromeを使っている方は、こんな警告画面を見たことがある人もいるかもしれませんね。ウイルスや危険なプログラムを配信しているWebサイトについて、Googleが検知したものはこのように告知してくれるようになっています。

とはいえ、全てのサイトについて警告してくれるわけではありませんし、このサイトは危険なのかどうなのか、何かあやしいんだけど、どうやって判断したらいいんだろうという事もあるでしょう。そういったときに目安として使えるサービスの一つが

(Webサイト調査・スライド2)

アグスというWebサービスです。今回は、実際にマルウェアに感染したWebサイトを、このアグスを使って調査してもらいます。大変危険な内容となりますので、最後まで話を聞いて作業をしてください。

まず、Google Chromeを使って、スライドに表示している www.aguse.jp にアクセスします。

(作業してもらう時間)

アグスWebサイトは開きましたでしょうか。開いたら、次に

(Webサイト調査・スライド3)

このWebサイトのアドレスを、アグスの「調べたいサイトのURLを入力してください。」という下の部分に、入力してください。http:// という部分も忘れずに入力しないと、正しい結果が出ないので注意してください。

(Webサイト調査・スライド4)

このWebサイトの管理者の方には、事前にこのような警告が出ている件について連絡しているため、既に対応されていた場合はマルウェアが検出されないかもしれません。

もしWebサイトが何らかのマルウェアに感染していた場合、この画面のようにマルウェア感染が通知されます。下の方にスクロールしてもらうと、そのWebサイトが様々なブラックリストに載っていないかどうかも調べてくれるので、あわせて確認しておきましょう。マルウェア感染だけでなく、フィッシングや迷惑メール送信業者、詐欺サイトのブラックリストに載っていないかどうか確認できます。

ただ、こちらのサイトで何の問題も出ていないけれど、やっぱり何かあやしい、とか、アグスではカスペルスキーというウイルス対策メーカーのチェックだけなので、他のウイルス対策メーカーでもチェックしたい、ということがあるかもしれません。

その場合には、次のサイトが役に立ちます。

(Webサイト調査・スライド5)

ヴァイラストータルというWebサイトです。こちらのサイトは、2012年にGoogleが買収したサービスですが、複数のウイルス対策メーカー製品で、あやしいファイルやWebサイトのチェックができるという、有名なサービスです。

こちらのサイトでも、先ほどのサイトを調査してみましょう。まず、このスライドに表示しているvirustotalのサイトのアドレスを、Google Chromeに入力して、Webサイトを開いてください。

(Webサイト調査・スライド6)

virustotalが開いたら、URLというタブを押して、その下の入力する部分に、再度この感染サイトのアドレスを入力してください。

そして、スキャンするという青いボタンをクリックすると、「分析済みの URL です」という表示がされたと思います。以前に私の方で一度チェックした結果が残っていますので、右下の「前回の分析結果」をクリックしてください。

(Webサイト調査・スライド7)

すると、このスライドのような結果画面が表示されると思います。61個のウイルススキャナーの内、3つで危険なサイトだと判断されていますね。数だけで言えば少ないと思いそうですが、1つでも検出されていると、危険だと判断して、アクセスを避けるのが賢明です。

ちなみに、Unrated siteという灰色の文字がいくつかありますが、これは「評価対象にしていない」という意味で、あやしいかどうか判断しないよ、ということになります。

余談ですが、本来ここでは詐欺サイトの調査を色々とやってもらう予定だったのですが、既にネット上から消えてしまっていたので、題材をこちらにしました。そちらは楽天に似せた詐欺サイトで、ポイント10倍と書いているのにポイントシステムのようなものが無いとか、ドメインを調べたら中国のレジストラで中国人の名前で取られていたとか、サーバーはアメリカにあるとか、あやしい要素が満載でした。

詐欺サイトに良くあるのは、価格が相場と比べて安すぎる、https が使われていない、支払い方法が銀行振込のみ(最近はクレジットカードの情報を盗む目的で、クレジットカード対応しているところもあるので注意)、銀行の口座名義が日本人のように見えない(ワン、チャンなど)、Webサイトの日本語がおかしいなど、チェックポイントがいくつかあるので、良く確認してから購入するようにしてください。

(ラストスライド)

最後にまとめです。このまとめは、ある海外のテレビ番組で放送された内容をまとめた物でもあるのですが、詐欺や危険から身を守る3つのポイントです。

ひとつめ、これは最初に話した内容と通じますが、詐欺やあなたを騙そうとする人は、信じるという心の動きを利用します。そして、信じるという心の働きには個人差があり、信じたいと思うものを信じるようにできています。ですから、信用する前に、それが信ずるに足るものか、他の手段で必ず確認するようにしてください。今回の講義で言えば、最後に行ったWebサイトの調査がそれにあたるでしょう。

ふたつめ、危険にあわないためには出歩かないこと、当たり前ですが家の中より外の方が危険です。しかし、家から出ない、すなわちネットを使わないというわけには、今どきいきませんよね。ただ、使う回数や時間を絞ったり、安全という確信が持てるサイトを見るだけとか、使い方を工夫すれば危険にあう可能性は減らせます。ただ、最近は昨日まで安全だったサイトが乗っ取られ、危険なデータをまき散らすこともありますから、一概に安全なサイトだけ見てればいいというわけにもいきませんが・・・。

危険なサイトは、一般にPCを標的にしていることが多いので、スマートフォンやタブレット端末で閲覧するようにすれば、多少は危険を減らせるかもしれませんね。これも弱い部分の露出を減らすという、一つの防衛方法です。ただ、Windowsタブレットは多くがWindowsそのままの端末なので微妙ですし、Androidは比較的セキュリティが弱いとか、色々と気にする部分はありますが・・・。

みっつめ。何より身を守るには、知識を持つことです。「敵を知り己を知れば・・・」という有名な孫子の言葉がありますが、これは本当にその通りです。概要だけではなく、実際に起こった事件や攻撃を知ることで、身を守ることができます。ネット上ではそういうセキュリティに関する情報はたくさんありますから、興味があればぜひ色々と調べてみてください。

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と、まとめきれなかったセキュリティ情報などトーク)