セキュリティインシデントとその対策

2005/8/29

本書は、医学部において「セキュリティインシデントとその対策」と題して行った講演をまとめたものです。講演は同じ題 目で 2 回(2005/07/12,28)行いましたが、それぞれ独立したものです。しかし、その内容は 1 部重なりますので、本書では 2 つの公演を 1 つにま とめました。

今回は、一般ユーザの立場で、セキュリティインシデントに対してどのように対応すべきか、についてお話をさせていただきます。

ネットワークのセキュリティを確保するためには一般にはファイアウォール、IDS(Intrusion Detection System) 、ウィルス対策ソフト、通信路の暗号化(VPN 等)のセキュリティ技術の導入が必要といわれていますが、このようなことはネットワーク管理者等の専門家の 仕事であり、皆様には直接の関係はありません。しかし、このことは皆さんがセキュリティについてまったく無関心でいいということでありません。最近、セキュリティ技術の導入だ けではどうしても限界があるということがハッキリしてきました。それはどういうことかといいますと、セキュリティ技術だけでは守り切れないということ、そ れから一般のユーザの配慮に欠ける行動が大きな災難を大学のネットワークに

招きいれてしまう可能性があるということです。

皆さんはファイアウォールという言葉を聞いたことがありますか。ファイアウォール(fire wall)とは、もともと防火壁という意味です。火事があったときに延焼を食い止めるための壁ですね。この言葉がネットワークセキュリティの分野に持ち込 まれて外部からの侵入を食い止めるための壁という意味で使用されるようになりました。火事を食い止めるためのファイアウォールと、インターネットからの侵 入を食い止めるためのファイアウォールには決定的に違う点があります。火事を食い止めるためのファイアウォールは、全てのものをシャットアウトします。延 焼を食い止めるには空気の流れを遮断する必要があります。したがって、ファイアウォールは空気を通してはなりません。空気を通してはならないということ は、何も通さないということだと思ってください。これが従来のファイアウォールです。しかし、ネットワークを外部から守るためのファイアウォールは、イン ターネットとの間を完全に遮断してしまうと使い物になりません。インターネットは現在、社会インフラになりつつあるといっても言い過ぎではないでしょう。 電気や水道、ガス、電話などと同じで、インターネットがなくては社会生活が成り立たなくなりつつあります。特に企業における経済活動は完全にインターネッ トに依存しているといっても言いすぎではないでしょう。そこで、ネットワークで使用するファイアウォールは、ネットワークを流れるパケットを監視し、ある ものは通過させ、あるものはブロックするということになります。もう少し具体的な話をしましょう。これ以降はファイアウォールという言葉を、火事を食い止 める防火壁ではなくて、外部の侵入から内部ネットワークを防御するためのシステムという意味で使うことにします。

ファイアウォールはネットワークを外部ネットワークと内部ネットワークに分けて、外部ネットワークは信頼性に欠けるネットワーク、内部ネットワークは信 頼できるネットワークと考えます。信頼性に欠ける外部ネットワークとは、とりあえずインターネットのことだと考えていいでしょう。信頼できるネットワーク とは社内ネットワークあるいは、大学内ネットワークです。しかし、社内ネットワークでも人事部や、財務部のネットワークを他から引き離してファイアウォー ルで守るということも当然あります。大学のネットワークでも事務部門を、研究・教育ネットワークと切り離してファイアウォールで守ると

いうことが当然あり えます。しかし、ここでは簡単のためにそのような細かいことは考えないことにしましょう。

ネットワークを信頼の欠ける外部ネットワークと、信頼できる内部ネットワークに分割して、その間にファイアウォールを設置します。そして、外部ネット ワークと内部ネットワークとの通信は必ず、このファイアウォールを経由するようにネットワークを設計します。誰か不心得者がいて、ファイアウォールを経由 しないでも外部ネットワークにつなげるようにしてしまうとこの作戦は台無しになってしまいます。ネットワーク管理者に無断でネットワークに穴を開け、ファ イアウォールを回避して外のネットワークに接続することは絶対にやらないでください。ファイアウォールにはさまざまな仕組みがありますが、細かいところを 理解するためには、皆様がインターネットの仕組み(勉強したい人は手始めに TCP/IP について学ぶ必要があります) に精通している必要がありますので、今回は大雑把な話だけにします。インターネットはパケット通信と呼ばれる通信方式を採用しています。パケット通信と は、送りたいデータを小さく小分けにして送る方式です。パケットとは、Packet と書きます。小包とか、小荷物などという意味です。データを小さく小分 けして、そのデータに送り主や、宛先などを書きます。宛先は、「何々国何々県何々市何丁目何番地ドコドコビルの何階の何とか会社の何とか部何とか課の誰々 様」という感じになるでしょうか。この送信元や宛先の情報などを基準にして、このパケットは送信しよう、このパケットは破棄してしまおうという取捨選択を 行います。この選択基準はポリシーとして設計します。送信元が「何々国何々県何々市」だと危ない、あるいはもっと詳細に「何々国何々県何々市何丁目何番地 ドコドコビルの何階の何とか会社」だと危ないなどということを事前によく調べてポリシーを設計しておきます。ここで、「何々国何々県何々市何丁目何番地ド コドコビルの何階の何とか会社」というのは通常は IP アドレスと思っていただいていいと思います。IP アドレスについては皆様ご存知と思いますが、133.100.20.5 などというドットで区切った 4 つの 10 進数の並びですね。ですから、送信元の IP アドレスが 20.10.*.*であるものは全部 だめとか、IP アドレスを最後まで指定して、その特定の IP アドレスのものだけだめとか、などさまざまな手法が考えられます。「何とか部何とか課の誰々 様」というのは、イメージ的にはメールとか、Web などです。これらはアプリケーションといいますが、各アプリケーションは名前

を持っています。名前だけ でなく、ID も持っています。組織に属している人は通常、ID 番号を持っていますね。社員番号とか、ID 番号などとよばれます。この ID 番号を、アプリ ケーションも持っています。アプリケーションの ID 番号は通常ポート番号と呼ばれます。メールであればポート番号 25、Web はポート番号 80 などです。 メールは 25 番だけではないのですが、細かいことは省略します。ファイアウォールもこのポート番号を使って取捨選択をします。どのポート番号のアプリケー ション通信を許可するということを通常ポートを開けるといいます。Web を許可する場合は、ポート番号 80 を開けるということになります。

ファイアウォールには大雑把に言うとフィルタというタイプと、Proxy というタイプがあります。 細かいことをいうと、その中間的なタイプもあって通常サーキットタイプというのですが、今回は省略します。フィルタというのはパケットを通過させるか通過 させないかです。ある会社に行って総務部の A さんに会いたいとします。守衛さんはあなたのことをいろいろ調べて、OK ならば、あなた自身が総務部の A さん のところに直接会いに行くことを許されたとしましょう。これは、フィルタと呼ばれるものと同じです。もし、守衛さんがあなたの用件を事こまかく聞いて、守 衛さんがあなたの代理となって、総務部の A さんのところに行き用件を済ませてくれたとしたら、これは Proxy と呼ばれる仕組みと同じです。これは、外部 ネットワークから内部ネットワークへの通信のたとえですが、実際は内部ネットワークから、外部ネットワークへの通信もあります。無理やり今のたとえ話を拡 張してみましょう。フィルタだと外出時に守衛さんの許可を得て外出するということになります、Proxy だと外出したいときは守衛さんに代理を頼んで外回 りの仕事は守衛さんに頼むということになります。守衛さんの仕事はものすごく大変なものになります。ファイアウォールはこれくらい大変な仕事をしていると いうことになります。こんな大変な仕事をしている守衛さんは世界中探してもたぶんいませんので、たとえ話としては成功していないと思いますが、ファイア ウォールのイメージは持っていただけたかと思います。

簡単に言うとファイアウォールというのはどこかのポートが開いているということです。大体、どの組織でもメールと Web だけは最低限使える状態にしてい ると思います。そうでないとネットワークが使い

物になりません。だとすれば、通過を許されたパケットに成りすまして、ファイアウォールを通り抜けることも 可能だということも分かるでしょう。先ほどの会社の守衛さんの例で言うと、偽造した社員カードを使って社員に成りすますとか、協力会社の社員や、取引会社 の社員に成りすますなどしてチェックを通り抜けるということです。

大抵の組織はメールを通過させるようにファイアウォールのポリシーを設計しているといいました。会社の守衛システムでいうと、メールは正社員のようなも のでしょうか。正社員は社員カードを提示すると会社の建物に入ることができます。正社員のスーツのポケットにハムスターが入っていると一緒に建物に入るこ とができます。いくらペット好きだからといって、ハムスターと一緒に会社に行けるとしてもそれほどうれしくはないでしょうが、まあそういうことです。メー ルの場合は、ハムスターに当たるのは添付ファイルです。メールが素通りだとすれば、添付ファイも素通りです。したがって、メールの添付ファイルにいろいろ 悪さをするプログラムを仕掛けておけば、悪いことができるということになります。皆さんはウィルスをご存知だと思います。ウィルスの殆どがメールに添付さ れる形で内部ネットワークに侵入してきます。かといってメールをブロックするわけにもいきません。

ところで皆さんはスパムという言葉を聞いたことがあると思います。スパムとは、もともとは、ハムのようなソーセージのようなコンビーフのようなやわらか い肉の缶詰のことです。このスパムを販売している会社が「スパム！ スパム!・・・」と連呼するテレビコマーシャルを流していたということですが、そのス パムのテレビコマーシャルのごとく、人の迷惑も顧みずに大量に送信されてくるメールをスパムとか、スパムメールといいます。スパムは、別名 UCE (Unsolicited Commercial Mail)といいます。「solicit」とは、歓迎するという意味ですので、「歓迎されざる商用メール」ということになります。受け取る人の迷惑を考え ずに勝手に送られてくるメールということですね。スパムメールは、多くの場合、不誠実な商法や、製品、ポルノサイトの紹介と関係していますが、ウィルスに も関係しています。そのほか、今日お話する多くのことに関係しています。

ウィルスは大抵の場合、メールに添付されてくるといいましたが、

多くの場合そのメールはスパムメールです。したがって、ウィルスをブロックするには、ウィルスそのものに焦点を絞って対策を講じると同時にスパムに対する対策も重要だということになります。

　初めにウィルスのブロックの話をします。ウィルスはメールに添付されて内部ネットワークにやってくるといいました。もちろん、FD に感染して入ってくる こともありますが、今回はメールの話に限定します。メールに添付されてくるが、メールの仕組みを止めるわけにはいきません。そこで、添付ファイルを調べ て、ウィルスが添付されているかどうか検査するのが、一般的なウィルス対策です。通常の場合は、ウィルスが持つ特徴を研究して、ウィルスの特徴を持つもの を選別してブロックします。つまり、ウィルスのパターンの研究ということになります。いちいち、添付ファイルを検査して、悪さをするかどうか動作試験をす るというのでは大変ですので、ウィルスの特徴を持っているものはウィルスと認定し、ウィルスの特徴を持っていないものはウィルスではないと認定するので す。つまり、実際にウィルスであっても、ウィルスの特徴を持っていないものはウィルスとは判定されないということです。ウィルスのパターンは定義ファイル というデータベースにまとめられて、それを辞書代わりにしてパターンチェックをするわけですが、出来立てのウィルスのパターンは定義ファイルのなかに記述 されていませんので、ウィルスと判定されない恐れがあります。ウィルスは毎日毎日、世界中のどこかで新しいものが作られていますので、定義ファイルは日々 更新されなくてはなりません。つまり、定義ファイルの更新は、ボランティアの仕事ではできないということです。インターネットの多くの仕組みは世界中にい る優秀な技術者、研究者、プログラマがボランティアの形で作ったものが多いのですが、ウィルスはボランティアの力では防御できそうにありません。事実、ア ンチウィルスとかウィルスチェッカーとか呼ばれるものは殆どが商品です。では、アンチウィルスをどこにインストールすればいいでしょうか。当然メールの通 り道の置くわけですが、どこでしょうか。メールは、メールサーバというものを介して送信され、メールサーバ上のメールボックスというところに配信されま す。名宛人は、そこにメールを取りにいきます。メールサーバを介してメールを送信する仕組みを SMTP といいます。メールボックスにとりに行く仕掛けでは POP というプロトコルが代表的です。したがって、そのどこかにウィルスをチェックするプログラムを仕掛けておけばいいということになりま

す。あるいは、 ユーザのパソコンに仕掛けることも可能です。そのうちの全部に仕掛けるのは大変ですので、ネットワークの表玄関に当たるメールサーバと、各ユーザの使って いるパソコンに仕掛けておくのがいいでしょう。通常のアンチウィルスシステムは、ユーザ何人に対していくらという価格設定になっていますので、ユーザ何千 人などという組織では出費が大変です。しかし、現状では必要経費と考える以外ありません。

ところで皆さんのお宅では、ウィルスはチックしていますか。大学でいくら高いお金を出してウィルスをブロックしても、皆さんのお宅のパソコンがウィルス に感染し、そのことに気がつかずに、そのパソコンを大学のネットワークに接続したら、あるいは FD や、USB メモリ等を介してウィルスを大学に持ち込んだ りしたら、それこそ台無しです。ぜひ、皆さんのお宅でもウィルスをチェックしていただきたいと思います。

さて、今度は Web の話にいきたいと思います。Web はキラーアプリケーションと呼ばれることがあります。インターネットの初期は、メールをいかにして 使いやすいものにするかということに開発のエネルギーが注ぎ込まれたといっていいでしょう。初期のインターネットは研究者のためのネットワークでしたが、 やがて一般のユーザが参加して爆発的な発展を遂げることになりました。そのきっかけとなったのが Web の開発です。Web もインターネットでは欠かせない アプリケーションです。Web もファイアウォールでブロックしにくいアプリケーションです。先ほど、メールの話をしましたが、メールの場合は、外から中に 入ってくるメールも、中なら外に出て行くメールもともにブロックすることはできません。もちろん、理論上、技術上できないという意味ではなく、社会活動、 経済活動の必要上できないという意味です。しかし、Web はちょっと話が違います。インターネットのアプリケーションは通常クライアントサーバシステムと いう方法で機能します。クライアントサーバシステムとは、クライアントから積極的にサーバに対して働きかけるシステムです。サーバには Web のコンテンツが入っていてクライアントからの要求にしたがって、データを送ります。通常の Web の使い方では、インターネット上にある Web サーバに対して、内部ネッ トワーク上のクライアントから要求に行きますので、Web 通信に対する通常のポリシーは内から外へのパケットは許可するが、外から中へのパケットは許可し ないというものになります。イン

ターネットの通信では、サーバとクラインとがデータを交換しますので、クライアントからの積極的な要求に対するサーバから の応答も、外から内へという方向でやってきますが、ファイアウォールはこのようなパケットは見分けて通すことができます。いま、「通すことができます」と いいましたが、実際には、「通すように設定しておく必要がある」といった方が正しい言い方です。

Web を使う場合は、内部ネットワークから外の Web サーバに接続するのは通常許可されます。あるいは、皆さんのお宅ではどうでしょうか。皆さんの中に は、自宅でも LAN を張っている人がいるかもしれませんね。あるいは、パソコン 1 台だけで ISP に接続しているかもしれません。皆さんのお宅では、Web は使えますよね。インターネットに参加した目的はたぶん Web とメールを使うということでしょう。お宅から外のインターネット上の Web サイトは見られま す。しかし、皆さんのお宅では Web サーバは起動していますか、たぶん多くの方は Web サーバを立てるなどということはしていないと思います。したがっ て、インターネットから皆さんのネットワークに Web で接続してくることはないでしょう。インターネット上から、皆さんのお宅に接続できないということは 一応安全であるといえるのですが、そうとも断定できないことがあります。飛んで火にいる夏の虫という言葉がありますが、これです。インターネット上には、 警戒心の薄いユーザが引っかかりそうな罠を仕掛けてじっと待っている Web サーバがあります。通常、フィッシングなどと呼ばれます。これなどは、内から外 への接続ですので、通常許可されます。そして、まんまと罠に引っかかることになります。銀行やクレジット会社のサイトとまったく見分けがつかないようなサ イトを作って、じっと待っています。しかし、じっと何もしないで待っていても、自分からそんなサイトに行って罠に引っかかるおめでたい人もあまりいないで しょう。多くの場合、スパムメールが使われます。片端からメールを送信して、たとえば「何々銀行です。このたび、システムの変更をしましたので、ユーザの 皆様には再度、アカウントの ID 番号の入力をしていただきたいと思います。」などとまことしやかにメールします。たぶんこんなんでは誰も引っかからないで しょうが、向こうは詐欺師ですから、もっとうまい言葉を考えつくはずです。そのスパムには、たぶんその銀行を装った罠の Web サイトへのリンクが仕込まれ ています。うっかりリンクをクリックしてしまうと、大変です。ID 番号が盗まれれば、ID カードが偽造されてしまいます。このような怪しいメールを受け 取ったらその銀行の窓口へ自

分で電話する、あるいはブラウザのアドレスバーに自分でその銀行のURLを入力するなどの注意が必要です。

ウィルスもスパム、フィッシングもスパムが手段として使われます。これでスパムに注意することが大切だということがお分かりかと思います。それと最近や かましく言われている個人情報の取り扱いです。個人情報が漏れて、その情報を手がかりにしてフィッシングを仕掛けられることも大いにありうることだからで す。

個人情報、個人情報というがどうしてそんなにやかましく言うのかと思っている人も中にはいるかも知れませんが、最近のオレオレ詐欺の実態を見れば、個人 情報の大切さが実感できるでしょう。フィッシングは、インターネット版オレオレ詐欺といわれています。皆さんの中に学内でWebサイトを運営している人も いるでしょう。Webサイトで不用意に個人情報が漏れていないかもう一度良く注意していただきたいと思います。例えば、秘匿情報を削除せず黒塗りしただけ のテキストがWeb上で公開されていることはないですか。その黒塗りした情報は検索にヒットしませんか。あるいはExcelの非表示操作をしただけの資料 はありませんか。IE(Internet Explorer)からHTMLコードを表示すれば(「表示」→「ソース」メニューの選択)見えてしまいます。それからメールについて言い忘れましたので ここで付け加えておきます。大勢の人に一斉にメールをするとき、CCを使いますが、CCで書いた宛先は名宛人全員に見えてしまうことは分かっていると思い ます。例えば、外部の人にメールする場合、それでいいのかはその都度判断していただきたいと思います。CCのメールアドレスを見せたくないのなら、Bcc を使ってください。個人情報に関しては、大きな問題ですので、最後にもう一度お話しします。

次にスパム対策について話をします。スパム対策もウィルスチッカーなどと並んで、セキュリティベンダーの儲けのたねになっていますがとりあえず、皆さん とはあまり関係ありません。最近では、一般ユーザ向けのセキュリティ製品でウィルスにも、スパムにも対応しているものもありますが、とりあえずここでは無 視します。スパムというのは、メールですから、当然メールアドレスをつけます。このメールアドレスはまったくのでたらめで、自動的にアドレスを作成して、 手当たりしだいに送信するということもあります。「このメールを受け

取りたくない人は、ここに返信してください」などと書いてあったら、絶対に返信をしな いでください。うっかりそこに断りのメールを送ってしまったとしたらあなたは、相手の罠に引っかかったということになります。彼らは、そのメールが相手に 届くかどうか半信半疑なのです。しかし、返信メールを送ってきた相手には確実に届いていたことを確信します。彼らは、どうするでしょうか。あなたのメール アドレスは確実に届くメールアドレス、つまり「脇の甘いユーザのリスト」として、スパマー(スパムメールを送る人)の間で引っ張りダコということになりま す。そのあと、いろいろのところから大量のスパムメールを受け取ることになるでしょう。

もちろん、スパマーも、自動で作った、届くかどうかわからないメールアドレスよりも、確実に届くメールアドレスを欲しがっています。では、どんな手段 で、メールアドレスは収集されるのでしょうか。メールアドレスの入っている顧客リストなどは高価で取引されています。あるいはロボットを使って Web サイ トから収集してきます。スパマーに売ることを目的としてユーザのメールアドレスを収集している Web サイトなどもありますので要注意です。無料でハワイ旅 行にいけるなどという誘い文句につられて、不用意に自分のメールアドレスを入力するなどということがないように注意してください。宝くじサイトなども要注 意です。アンケートに答える(それとなくメールアドレスも聞いてきます)と何かがもらえるなどというのは怪しいと思わなくてはなりません。とにかく、得体 の知れない Web サイトにいって、言われるままにメールアドレスを入力するといった軽はずみな行動は慎んでください。ホームページで自分のメールアドレス を曝しておくことなども気をつけてください。どうしても、必要ならば自分のメールアドレスをイメージファイルとして保存して、それを画像ファイルとして呼 び出しておけばいいでしょう。メールアドレスを入力する必要がある場合は、偽のメールアドレスを使ってください。相手から確認のメールを受け取る場合は、 偽のアドレスではだめですので、このような場合のために、使い捨てのメールアドレスを用意しておくのもいいことです。

まだまだスパムに絡んだトラブルがあります。たとえばスパイソフト、あるいはスパイウエアなどと呼ばれているものがあります。スパイソフトとは、ユーザ に気づかれないようにパソコン内の情報や活動の記録を、ソフトウエアの開発元に送信してしまうソフトです。この

スパイソフトがウィルスに添付されてやって くることが多いのです。ウィルスはスパムメールに添付されてということになります。何が盗まれるんでしょうか。たぶん、パスワード、クレジットカードの ID 番号、クッキー(Cookie)などです。

皆さんは、クッキーって知っていますよね。もちろんおやつじゃありません。皆さんは Web サイトに入って抜けるまでにいろいろのことをすると思います が、その際に最初にアカウントとパスワードを入力するだけだと思います。Web プロトコル、プロトコルというのは通信の手順のことですので、Web プロト コルとは、Web アプリケーションを利用する際の通信手順です。この Web プロトコルは本来すごく単純にできていて、クライアントからの要求に対して、 サーバが応答するという 1 組のパケットのやり取りで接続が終了します。したがって、Web サイトに入ったままでも、何かするたびに別の接続を確立していま す。しかし、接続のたびにいちいちパスワードによる認証をしていたのでは面倒でしょうがないので、一度 Web サイトに入ったときに認証を行い、一度認証し たクライアントにはサーバから Cookie というデータを渡します。俗に、「クッキーを食べさせられる」といいます。そして、次の接続でクライアントが Cookie つきのパケットを送信すると認証の手続きを省略してくれるという仕掛けです。現在の Web プロトコルは少し複雑になり、一回ぽっきりで接続が 切れてしまうということはないのですが、細かい話は省略します。Cookie は最初の認証の際に、サーバがクライアントマシンに格納します。したがって、 Cookie を盗まれると成りすましにあう可能性があります。Cookie が盗まれると、あなたのふりをしたクラッカーに大量の買い物をされ、法外な料金 の請求をされる恐れがあります。
IE6.0 では、Cookie の取り扱いをいろいろと制御することが可能ですのでやってみてください。

Cookie やクレジットカードの ID などを盗まれるのは、フィッシングや、スパイソフトだけではありません。P2P というソフトウエアもたびたび問題を引き起こしています。

P2P とは何でしょうか。P2P はネットワークを越えてファイルを検索したり、ファイルをコピーしたりするソフトです。皆さんの記憶に新しいところでは Winny などというプログラムがあります。P2P とは Peer

to Peer ということです。Peer とは、年齢あるいは地位が同等の仲間という意味です。これはクライアントサーバシステムと対極にある考え方です。現在の インターネットサービスは大部分が、クライアントサーバという考え方で作られています。クライアントサーバシステムとは、クライアントとサーバの関係は、 クライアントがアクティブで、サーバがパッシブです。クライアントはアクティブにサーバに対して接続要求を行います。サーバはあくまでパッシブです。クラ イアントからの要求があるまでは決して行動に出ません。クライアントからの要求があればそれに応じて必要な動作をします。大まかに言えばこれがクライアン トサーバシステムです。ところが P2P はどれがサーバやら、クライアントやらはっきりしません。P2P にもいろいろのタイプがあります。ありますというよ りも、P2P は開発当初からセキュリティ、法律上の問題を指摘され、それを避けるため形を変えてきたといっていいでしょう。現在の形は、どれがサーバやら クライアントやらはっきりしません。あるときはクライアントのように振る舞いあるときはサーバのように振舞います。現在のセキュリティ製品はクライアントサーバシステムに対して対応するようにできていますので、P2P は困った存在です。現在の、P2P ソフトは、P2P ソフトの間をバケツリレーのようにして コピーしたファイルを転送していきます。P2P は、今まで話題に上ったものと決定的に違うのは、P2P ソフトは自分の意思でパソコンにインストールするこ とが多いということです。P2P はサーバとクライアントの役割をうまく使い分けながら、パソコンからパソコンへのファイルを転送していきますので、P2P で使用するポートを開けておく必要があります。ポートについては、最初に話題にしたファイアウォールのところで説明しました。あのポートです。自分の意思 で P2P をインストールしますので、自分の意思でポートを開けるということもつじつまがあいます。自分でポートを開ける必要がありますので、たぶん大学や 会社の中では使えないでしょう。しかし、自分のパソコンに入れるのなら問題はありません。セキュリティ上からは問題は大有りなのですが、ここで問題なしと いったのは、インストールして、ポートを開けるということに対して、それを止める人はいないという意味です。その人のパソコンなのですから。でも、それで いいのでしょうか。P2P をインストールしていたためにパソコンに入れていた個人情報が流失してしまったという事件が起きています。クレジットカードや、 Cookie が流失してしまう恐れも当然あります。P2P 型のウィルスというのも出てきています。もちろん何度も言っているように、こ

の P2P 型のウィル スもスパムメールに添付されてくる可能性が大です。

次は、DoS の話をします。DoS と言ったってもちろん MS-DOS のことじゃありません。DoS とは Denial of Service という意味です。日本語に訳すとサービス停止ですね。サービス停止攻撃です。これは実に厄介な攻撃です。なぜかというと DoS 攻撃を仕掛け てくる輩はなにも欲していないのです。ただ、標的とするネットワークに迷惑が及べば喜ぶというなんとも性質の悪い攻撃です。ファイアウォールは不正に侵入 してくる攻撃に対しては防御できるのですが、DoS は侵入してくるわけではありません。DoS は、ネットワークの帯域や、CPU やメモリや、あるいは接続 を確立するときに使うバッファというメモリを一時的に使い切ってしまう攻撃で、これらの個々の動作は別に悪いことではありません。たとえば、ネットワーク の外からメールを大量に送信して、サーバをシステムダウンに陥れる行為がありますが、メールを送信する行為自体は別に悪いことではありません。この行為 は、高速道路で乗り込んできた暴走族の行為に似ています。DoS にはこれといって決め手になる防御策がありません。また、DoS 型のウィルスというものも あります。もちろん、このウィルスもメールに添付されてやってきます。たぶん、メールはスパムです。

ここまでセキュリティ上の脅威についてさまざまなことをお話してきましたが、不正侵入については話題にしていません。最初にファイアウォールのお話をし ました。そして、世間ではファイアウォールさえあればセキュリティは守れると勘違いしている方も多いと思いますが、ここまでお話したセキュリティ攻撃は不 正に侵入することなしに行われるものばかりです。ネットワークに侵入しなくてもこんなに多くの攻撃方法があるんです。侵入してくれれば、しっぽを掴むこと も出来るんですが、残念ながら彼らもそんなに馬鹿じゃありません。クラッカーも不正侵入をすれば捕まるおそれがあるということを知っているのです。それに 彼らの目的は別に不正侵入して何かを盗んでやろうなどという大それたものではないのです。

しかし、クラッカーの立場からみれば、どうしても侵入しない限り目的を達成できないこともあるでしょう。その場合には、不正に侵入することになります。 もちろん、これは多くの場合、プロの犯罪者の仕業ということになります。こうなると、皆さんのような一般のユー

ザがどうこうするという問題ではありませ ん。ここはネットワークの専門家にまかせるしかありません。しかし、これらの犯罪のプロはいきなり侵入してくるなどという乱暴な手段に出ることはありませ ん。彼らは例外なく知能犯ですので、やることも慎重です。彼らは用意周到に準備をし、ネットワークに穴をあけ、しかも気づかれないようにしてその穴を大き くし、ネットワークに侵入し、目的を遂げて、侵入の形跡を消してから、去っていきます。ここでも皆さんの力添えが必要です。用意周到な準備とは何でしょう か。たとえば、皆さんのうちの誰かのパスワードを奪うことです。これがネットワークにあけた穴です。さらに穴を大きくするとは、トロイなどのプログラムを 仕掛けて管理者のパスワードを奪うことです。皆さんのパスワードは、ネットワークを守る石垣の１つの石に相当するかもしれません。１つの石が抜き取られる ことで石垣全体が破壊されてしまうかもしれません。皆さんの中に、自分の誕生日や、電話番号や、ID 番号をパスワードにしている人はいませんか。たぶんい ないでしょうが、もしいたら大変です。あなただけが自分のパスワードを誕生日にしていることと、大学の全員が自分のパスワードを誕生日にしていることとは セキュリティという観点からは殆どイコールだと思ってください。パスワードを紙に書いてどこかにしまってある人はいませんか。パスワードを付箋紙に書い て、パソコンに貼り付けている人なども何年か前にはいましたが、もうそんな人はいないでしょうが、注意してください。大切な情報が書いてある紙を無造作に ゴミ箱に捨てるなどの行為も慎んでください。クラッカーは侵入のために予備調査をするということを言いたいのですが、このあたりのことはいくら言ってもきりがないので、メディアセンターの Web サイトで確認してください。

　それから最後に個人情報の保護についてお話します。今年の 4 月 1 日(2005/4/1)から、個人情報保護法が施行されることになりました。今までの話 も、パスワード、ID 番号、メールアカウント、Cookie などの個人に関連付けられた情報を盗まれると「成りすまし」やカード偽造などの被害にあうこと になる、というものでした。しかし、丁寧に扱わなくてはならないのは、なにもパスワードや、ID 番号、メールアカウント、Cookie だけではありませ ん。また、情報もコンピュータの中に保存されたディジタルデータだけではありません。個人の名前、住所、電話番号、生年月日等の今までは無用心に取り扱わ れていたかもしれない情報がすべて個人情報として保護の対象になります。もち

ろん、今言いましたようにその情報はディジタル化されているか、紙ベースのも のかは関係ありません。このような情報の流出は「放っておいてもらう権利（プライバシー権の原型）」の侵害であることもさることながら、オレオレ詐欺(振 り込め詐欺)、架空請求、ダイレクトメールなどを誘発する恐れがあります。

最近の個人情報流失事件を眺めてみると、車上荒らしの被害にあって個人情報の入ったカバンごとそっくり盗まれたとか、個人情報の入った業務用のパソコン を電車の網棚に置いたまま居眠りしているときに盗まれたとか、あるいは個人情報のファイルを添付したメールを間違って違うメールアドレスに送信してしまっ たなど、不注意としか言いようのない事件が続出しています。もちろん、内部の人間が出来心で個人情報を盗み出し、名簿業者に売り渡してしまったという事件もあります。内部の人間は、正社員、パート社員、派遣社員、委託先の社員などさまざまです。

個人情報が漏れると、先ほども言いましたようにオレオレ詐欺(振り込め詐欺)や、架空請求、ダイレクトメールなどに使われるのはもちろんですが、大学自 体が事件に関わったとか、監督不行き届き等で損害賠償請求を受けることもありえます。また、社会的信用を落としてしまうことにもなりかねません。また、漏 洩事件を公にされたくなければ、いくらいくら払えなどという恐喝にあう恐れもあります。

個人情報保護は大学が一丸となって取り組むべき大きな課題ですが、個人情報を特に多く抱えているのが大学病院です。今回の講演会は、病院関係の皆様が対 象ですので、医療関係について若干説明させていただきます。個人情報の保護の関しては、衆議院の付帯決議で、医療・金融/信用・情報通信分野に関しては特 に高いレベルの個人情報保護が求められるとされています。これらの分野に関しては個人情報保護法では不十分なので将来は分野ごとの個別法が必要ということ ですが、とりあえず厚生労働省は、医療関係に関して個人情報保護法の規定よりも厳しいガイドライン(平成 16 年 12 月 24 日)をまとめ、各医療機関に対して、このガイドラインの線に沿って行動することを求めています。独立行政法人の医療機関は「独立行政 法人等の保有する個人情報の保護の関する法律」が適用されますので、直接このガイドラインの対象にはなっていませんが、ガイドラインの要求に十分配慮する ことが求められています。それでは、このガイドラインに沿って簡単に説明します。

●責任を負うのはだれか

　個人情報保護法では、個人情報取扱業者に対する義務が規定されています。従って、個人データの漏洩等の事件が起きた場合に責任を追及される恐れがあるの は、安全管理責任者や、監督義務者ということになります。しかし、このことは、個人は責任を問われないという意味ではありません。医師等の医療従事者は、 刑法や各資格法で規定される守秘義務違反に問われる可能性があります。また、資格を有しない従業者についても、業務の内容によっては、不妊手術、精神保 健、感染症などの関係法律によって規定される守秘義務違反に問われる可能性があります。なお、個人情報取扱業者でないものも、漏洩等によって権利を侵害さ れた者から民事上の責任を問われる可能性があります。

●個人情報取り扱いルール

個人情報取り扱いに関しては次のようなルールの遵守が求められます。

・保有の制限

　　利用目的の明確化。利用目的の達成に必要な範囲を超えて個人情報を保有しない。

・利用目的の明示

　　個人情報を取得するときは、利用目的を明示する

・利用および提供の制限

　　原則として、利用目的以外の目的に保有する個人情報を利用・提供しない

・正確性の確保

　　利用目的の範囲内で、保有している個人情報が過去・現在の事実と合致しているように努める

・安全確保の措置

　　保有している個人情報の漏洩などを防止するために必要な措置を講じる

・従事者の義務

　　業務に関して知り得た個人情報の内容をみだりに他人に知らせたり、不当な目的のために利用してはならない

●個人情報
個人情報とは何かですが、次のように定義されています。

氏名、性別、生年月日等の個人を識別する情報だけでなく、個人の身体、財産、職種、肩書き等の属性について、事実、判断、評価を表すすべての情報、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているか否かを問わない

死者に関する情報は含まれませんが、生存する遺族の情報が含まれている場合は保護の対象になりますので注意してください。たとえば、遺伝病でなくなった人の場合は、血縁者の情報がカルテ等に記載されているかもしれません。

●個人データ
個人データは、一定の規則に従って整理・分類され、必要な情報がすぐに取り出せるようになっているものです。

個人データは、特定の個人情報を検索出来るように体系的に構成した個人情報を含む情報の集合体

通常はコンピュータに保存されたデータベースということになりますが、紙で処理したものでも一定の規則に従って整 理・分類してあるものは個人データとみなされます。診療記録などは、媒体の如何を問わず、体系的に整理され、特定の個人情報を容易に取り出すことができる ので「個人データ」にあたることになります。

●暗号化されたデータ
ガイドラインは、個人情報に関して暗号化されているかどうかに関係ないとしていますが、これについては次のように考えてください。

暗号化により特定の個人を識別できないようになっていれば「個人情報」ではない

ただし、個人情報との対応表など、他の情報と容易に照合できて、そのことで特定の個人が識別できれば「個人情報」に当たります。

●医療機関の有する個人情報
医療事業者の保有する個人データとは次のような情報です。

患者・利用者の情報 医師、歯科医師、薬剤師、看護師、介護職員、事務職員等の情報 仕入れ先業者の従業者の情報

診療録・介護記録に記載された患者・介護者の家族に関する情報は、情報を記載されている家族本人の個人情報に当たります。

●死者の個人情報
　死者の個人情報に関しては先ほど説明しましたが、繰り返します。

死亡者の情報は個人情報保護法の対象にならないが、遺族の情報が含まれる場合は、その遺族の個人情報になる

●本人の同意
　本人の同意を得る方法については法律では明確化されていませんが、ガイドラインでは、文書による方法のほか、口頭、電話でも可としています。同意を求める内容や、緊急性等を勘案して、それぞれの場面で適切に処理することが求められます。

文書、口頭、電話による

　症例を学会等で発表する場合は、匿名化が必要です。匿名化が出来ない場合は、本人の同意をとってください。
　患者の数が少ない場合とか顔写真をつける場合など、氏名を隠しても特定の個人を識別出来てしまうので、匿名化できない場合に該当します。従って、このような場合は、本人の同意が必要になります。

●研究利用の場合の同意
　情報を匿名化し、「個人情報」に該当しない形で利用する場合は、同意は不要ですが、医学研究の分野では特に倫理指針が定められています。

情報を匿名化し、「個人情報」に該当しない形で利用する場合は、同意は不要

次の４つの医学研究の分野では、原則としてインフォームド・コンセントであるが、一定の条件がそろえばインフォームド・コンセントは必ずしも必要ないとしています。
・人ゲノム・遺伝子解析研究に関する倫理指針
・遺伝子治療臨床研究に関する指針
・疫学研究に関する倫理指針
・臨床研究に関する倫理指針

●患者の紹介医師からの要請
　患者の紹介医師からの診療記録提供の申し出をどう扱うかですが、利用目的をどのように考えるかがポイントです。患者本人への医療の提供に必要な範囲な ら、暗黙の了解があると考えることができます。紹介医師が研究のために利用するのであれば、黙示の同意があるとはいえないので、本人の明示的同意が必要と なります。

本人への治療の提供のためならば、黙示の同意があるものと考えることができる

●利用目的が明確な場合
　１８条第４項第４号(独立行政法人等の保有する個人情報の保護に関する法律では４条第４項)は、利用目的の明示に関して、取得の状況から見て利用目的が 明らかな場合は、利用目的を明示しなくてもよいとしていますが、ガイドラインでは患者への医療の提供に必要な利用目的だとしても院内掲示版等で公表すべき ものとしています。

患者への医療の提供に必要な利用目的だとしても、利用目的を分かりやすく示す観点から、院内掲示等で公表すべき

●患者の名前を呼ぶこと
　患者の名前も個人を識別できる「個人情報」ですので、患者から他の患者に聞こえるような形での氏名による呼び出しはやめて欲しいと

いう要望があれば、誠 実に対応する必要があります。しかし、患者の名前を呼ぶことが、患者の取り違えを防止するという面もありますので、患者の年齢、通院・入院の原因となる傷 病の種類などを勘案し、患者の希望も踏まえた上で、適切な対応をとることが期待されています。

●面会者への対応

入院患者から、面会等の外部からの問い合わせに回答しないで欲しいとの要望があった場合は、誠実に対応する必要があります。その患者が入院していること を前提に、面会に見えていることが明らかな場合は特段の事情がない限りは、案内してよいが、入院の有無を含めた問い合わせには応答しない方が得策です。

●個人データの第 3 者提供

個人データを第三者に提供する場合は、予め本人の明確な同意が必要ですが、場合によっては黙示的な同意でいい場合もあります。患者への医療提供として必 要の範囲内(23 条)の利用目的とみなすことが出来る場合は、院内掲示で公表し、患者からの明示的な留意の意思表示がない場合は、黙示の同意があったもの とみなすことが出来ます。たとえば、患者の家族への病状説明に関しては、患者の特段の同意を得ずに行うことを、院内掲示で公表しておけば、患者からの留意 の意思表示がない限り、患者に無断で行うことができます。ただし、この家族の範囲はどこまでなのか、予め患者に意思確認をしておくほうがいいでしょう。

23 条の第 1 項 2 号は、「人の生命、身体または財産の保護のために緊急の必要性がある場合であって、本人の同意を得ることが困難であるとき」は、予め本 人の同意を得られなくても、個人データを第 3 者に提供できるとしています。これは、予め本人の同意を得られないままで、本人が人事不省の状態に陥った場合 を想定していると思われますが、本人が明確に、個人データの第 3 者提供を拒否している場合はどうでしょうか。問題になるのが、未成年の患者の妊娠、薬物乱 用、自殺未遂等の秘密など、親に内緒にして欲しいという要望がある場合です。本人または家族の生命、身体または財産の保護のために緊急の必要がある場合 は、本人の意思に反して、家族に病状の説明をすることは可能です。しかし、未成年といって親とは独立の人格がありますので、一定の配慮は必要でしょう。あ とは、個々の具体的な事例にお

いて、患者の症状等を考慮した医師の判断に期待することになります。

●災害時の対応

　災害時に患者の安否確認に対してどのように対処すべきでしょうか。災害時には、患者本人にも、その家族にも同意を求めることが出来ないという状況になる ことがあります。たとえば、患者本人が意識不明の場合や、患者本人の意識はあるが、災害時に病院が混乱状態で的確に外部からの問い合わせに対応できない場 合などに、どうしたらいいかです。

　家族または関係者と名乗るものからの安否確認に関しては、災害の規模等を勘案し、本人の安否を家族・関係者に迅速に伝えることで、本人や家族等の安心 や、生命・身体の保護等に資すると考えられるか否かがポイントになります。問い合わせの相手が、患者の身体的特徴を説明できるなど、家族と判断してもよい 場合は、詳細情報を提供することもできます。しかし、相手と患者との関係が十分に確認できない場合には、存否状況や怪我の程度等の限定的な情報提供にとど めるべきです。ただし、患者が身元不明である場合は、報道機関等へ情報を提供することが、患者を探し出そうとしている家族への助けとなります。このような 場合は、患者の同意なしの情報提供が認められるでしょうが、患者を探し出すための手がかりになる情報とはどんな情報なのかは、個々の事例によって医療機関 が判断する必要があるでしょう。

●診療記録は、医師の個人情報という面を持つ

　診療記録は患者本人の個人情報であると共に、その診療を行った医師本人の判断や評価の記録でもあります。しかし、診療記録全体が患者本人の保有個人デー タであるので、患者本人からの開示要求があった場合は、医師の個人情報という二面性があることを理由に診療記録の全部あるいは一部の開示を拒否することは できません。

●個人情報保護方針

　患者の個人情報の保護のついてどのような方針で臨むのかについては、各病院で「個人情報保護方針」定め、それを誠実の履行する必要があります。以下に個人情報保護方針の枠組みのサンプルを示します。

個人情報の収集について
　　医療の範囲での利用　→利用目的に関しては院内掲示
　　その他の目的に利用するときはあらかじめ了解を得る。
個人情報の利用および収集について
　　第３者提供について
　　患者の了解があった場合
　　個人を識別出来ないように加工して利用する場合
　　法令等で提供を要求された場合
個人情報の適正管理について
　　患者の個人情報を正確、適正に保つこと、患者の個人情報の漏洩、紛失、破壊改ざんまたは患者の個人情報への不正アクセスを防止するよう努める

個人情報の確認・修正
問い合わせ窓口
法令等の遵守と個人情報保護の仕組みの改善
　　個人情報の保護に関する法令、厚生労働省のガイドライン、医学関連分野の関連指針、その他の規範を遵守すると共に適宜見直しを行い、改善を図る

●プライバシー権
　プライバシー権は憲法 18 条(身体の自由)、１９条(内心の自由)などを元にして、肖像権、人格権の一部、または財産権であるパブリシティ権(自己の氏 名、肖像について対価を得て第三者に専属的に使用許諾する権利)などとして判例法上確立されてきた権利です。最初は、「放っておいてもらう権利」とか、「勝手にさせてもらう権利」などという消極的な権利としての面が強調されました。判例の積み重ねによって、徐々に積極的な権利としての側面が顕在化してき ていますが、情報技術の普及とネットワークの進化によりプライバシー権のとらえ方が決定的に変化し、最終的に個人情報保護という面では、成文法による保護 が必要と判断されるにいたったといっていいでしょう。

　判例の積み重ねによって、プライバシー権は判例法上の権利として確立されました。しかし、判例法は、あくまで事件が起きて裁判所が法律解釈を行う際に 「前例に倣う」という形で参照するだけの話です。

事件が起きていない状態で、プライバシー件を理由にして、自分の行動を裏打ちすることができません。たと えば、市役所に情報開示を求めることを考えてみましょう。市役所が自分の情報をどんな状態で把握しているのか、その情報に間違いがないのかなどを調べよう としても、判例法上のプライバシー権では対応できません。判例法上に認められたプライバシー権はあくまで、事件に巻き込まれた個人を保護する権利でしかな いのです。今日のようにインターネットの利用が盛んになり、個人情報の保護が叫ばれる時代になると、個人情報が危機に曝された後にそれを回復するための手 段としての判例法上の権利ではなく、個人情報が危機に曝されないように守る権利としての明文の規定が必要になったということです。

今回は、「セキュリティインシデントとその対策」というテーマで、一般ユーザがセキュリティ問題に対してどのように対応したらいいかについてお話をさせていただきました。

今までの話をまとめてみましょう。多くのセキュリティインシデントは不正侵入ではありません。不正侵入を行うためにはある程度の技術的な素養が 必要です。だれでも出来るという訳ではないんです。もちろん、全く技術的な素養なしに利用できる不正侵入用のツールがインターネット上にころがっているこ とも事実です。これらのツールを使う輩をスクリプトキディ(Script Kiddie)といいます。スクリプトキディが使うツールは予め分かっている脆弱性をターゲットとしますので、それらの脆弱性は事前につぶしておく必要が あります。スクリプトキディによるもの以外では、不正侵入はそれほど多くはないといっていいでしょう。クラッカーだって不正侵入をするのは、よくよく考え て侵入するしか方法がないという結論に至った場合だけです。一昔前は、侵入することで自分の技術力を世間に対して誇示するということもありましたが、自分 の将来を滅茶苦茶にするリスクまで犯して、自分の技術力を誇示するなどという馬鹿げたやつは今の時代にはあまりいないと考えていいでしょう。もちろん、こ のことで不正侵入に対する備えを怠っていいということにならないのは当然です。

しかし、多くの攻撃は侵入という大それた行動ではなくもっと気軽な行為によって行われます。そして、多くのセキュリティ技術が、これらの侵入以外の気軽 な犯罪行為には、あまり的確な防御策を提供していないのです。どうしてでしょうか。これらはメールや Web に絡ん

でいるとか、あるいは元々他人に迷惑をか けることだけを目的としているDoS攻撃だとか、自分自ら招いた災難であることが大部分だからです。メールやWebがらみのことは完全に防御すると自分の 手を縛ることになります。DoS攻撃自体は１つ１つの行為それ自体は適法行為であることが多いので、防御が難しいという面があります。それから、自分で罠 に引っかかるというのはツールではなかなか防ぐことが難しいんです。フィッシングの場合は自分から罠に飛込んでいます。スパイソフトはウィルスに乗っかっ てやってきています。ウィルスはメールに添付されてきます。メールは自分の意志で使っているシステムです。P2Pもたぶん自分でインストールしています。 最後は皆さん自身に返ってきてしまいました。もうこれは、皆さんに自覚をしていただく以外にはないということになります。

それから個人情報の保護に関しては、クラッカーの攻撃ではなく、大学の構成員の一人ひとりの普段の行動が問題になっています。

そこでセキュリティポリシーや、プライバシーポリシーを作って、それを守っていきましょうということになってきたわけです。これをセキュリティマネジメ ントといいます。もう、ネットワークのセキュリティはネットワーク管理者のような一握りの専門家だけで対応できる問題ではありません。今まで、ネットワー ク管理者は、自分の責任と思ってやってきました。現実には、夜もおちおち寝ていられないという状態で必死に頑張ってきました。でももう限界なのです。ネッ トワーク管理者だけでどうなるという問題を超えてしまったといっていいでしょう。是非、このことを理解していただいて一緒に協力して頂けるようにお願い致 します。今日は長い時間ご静聴ありがとうございました。

※）個人情報保護法のガイドラインにつきましては、平成16年度12月24日の厚生労働省の「医療・介護関係事業者における個人情報の適切な取扱のための ガイドライン」と平成17年3月(平成17年5月20日改定)の「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に関するQ & A(事例集)を参考にしました。