大学における情報セキュリティについて

by sakae kumehara skumehar@eng.gunma-u.ac.jp

2005/7/4

本書は、「総合情報メディアセンター」の開所式(2005/06/23)における講演の内容を加筆修正したものです。

本書は、ネットワーク/インターネット、システム等の専門的な技術知識を持たない読者を対象に情報セキュリティの説明をしています。しかし、情報セキュリティを専門技術の裏打ち無しに説明することは大変難しい作業です。読者の頭の中にインターネット等の技術的な基本知識がなくては説明そのものがむなしく空をさまようことになります。そこで、どうしても技術的な説明が必要な場合は、たとえ話をすることにしました。技術的な知識をお持ちの読者の方は、そのことでかえって話がややこしくなると感じるかも知れません。しかし、以上のような訳ですので、よろしくお願いいたします。

今回、「大学における情報セキュリティ」について講演させていただきます。従来、情報セキュリティは一握りのネットワーク管理者が人知れず頑張っていれば、それ以外の人々は情報セキュリティなどということは殆ど意識せずに日常生活を送ることができました。しかし、今日そのような牧歌的な生活は過去のものになりつつあります。ネットワーク管理者は、どんなに努力してもその努力は評価されず、何か問題が発生すると責任を問われます。非常に損な役回りです。それでもネットワーク管理者は何とかして、組織の情報セキュリティを守るために努力してきました。しかし、もうその努力も我慢の限界にきています。一握りのネットワーク管理者が頑張っているだけでは、もはやどうにもならないという時代になってしまったといっていいでしょう。

これからは、組織に属する構成員の一人一人が情報セキュリティにコミットしていかなくてはなりません。大学の構成員の一人一人が大学の情報セキュリティを守るための砦にならなくてはなりません。それは、情報セキュリティをマネジメントしなくてはならないと言うことです。今日は、なぜ情報セキュリティをマネジメントしなくてならないのかというところまでで、情報セキュリ

ティをマネジメントするためにはどうしなくてはならいないのかということまでは説明しません（本書では、講演の後に追加しています）。

目次

第１章　大学とセキュリティ

大学における情報セキュリティといっても一般社会における企業等の情報セキュリティとそれほど違うわけではありませんが、大学では「情報セキュリティ」を巡るトラブルが、一般社会よりもより鮮明な形で顕在化しており、しかも有効な対策がほどこされていないのではないかと考えられます。つまり、病気にたとえると一般社会と大学では同じような病気が蔓延しているが、大学ではその病状がより重篤で、しかも有効な対策が施されていないと考えられます。それはどうしてなのでしょうか。

■　大学の使命と情報セキュリティ

大学も、一般の企業も組織として「情報セキュリティ」が求められる時代になりましたが、大学で情報セキュリティを実現することは、一般の企業ほど簡単ではありません。それは、大学はただ単純に情報セキュリティを実現すればそれで済むという存在ではないからです。企業でセキュリティを実現しようとすれば、ただ亀のように頭や、手足を甲羅の中に隠して、ただひたすら外界との接触を断てば済みます。もちろんこれでは企業として経済活動を行うことはできませんので、外界との接触は必要ですが、それは必要最小限に限定することが可能です。

しかし、大学の本来の目的は社会貢献です。一般社会が大学の社会貢献として期待しているのが、大学内に保有される高度な知識を社会に還元してほしいということです。大学内の高度知識を社会に還元する方法としては、学生の教育、共同研究、情報発信などが考えられます。特に、経済的な理由で中央研究所などの組織を縮小している企業は、研究開発の軸足を大学との共同研究に移してくることが予測されます。また、地域の高校などが大学に対して情報発信を求めることが多くなるでしょう。しかし、一般社会は大学に対して、開かれた存在であってほしいと要望する一方で、情報セキュリティをしっかりしてくれと要求してきます。これはかなり矛盾した要求ですが、そんなことはできませんとはねつければ、大学は社会からそっぽを向かれてしまいます。従って、大学人はこの二律背反するような問題に解答を提示しなくてはなりません。

■　様々な構成員

大学は教員団、職員団、学生団などのグループによって構成されます。教員団は、大学の専任教員や外部の非常勤教員などから構成されます。教員は様々な大学を渡り歩いていくかもしれません。非常勤教員はいくつかの大学教員を掛け持ちしているかも知れません。また、学生団は毎年少しずつ入れ替わりま

す。このように様々な構成員の大学への帰属意識は一様ではありません。
何年か前までは情報セキュリティはネットワーク管理者等のスペシャリストが人知れず頑張っていればどうにか確保することができました。しかし、もはや一握りの専門家の持つ技術だけではとうていセキュリティを確保することはできないという状況になっています。組織の構成員全員が、セキュリティの意識を高めていく必要があります。その手段がセキュリティをマネジメントするという考え方です。様々な構成員からなる大学はセキュリティをマネジメントするという観点からは非常にやっかいです。一般企業などのトップダウン的なマネジメントになじむ組織は、セキュリティをマネジメントしやすいといえますが、大学のような複雑な組織にはセキュリティマネジメントは極めてなじみにくいといっていいでしょう。
大学のような組織でセキュリティをマネジメントするためには、構成員をひとつの方向に向けさせる何かが必要ではないかと考えます。それは、群馬大学をよりよい大学にするために頑張ろうとするなにかです。

■　様々な情報資産

大学には様々な情報資産があります。たとえば入試情報や、研究情報等です。入試情報には、入試要項のように公開を前提としているもの、過去の入試問題のように公開しても差し支えないもの、来年度の入試問題のように絶対に秘匿すべきものなど様々です。研究情報もまだ専門誌に公開していないもの、特許取得前のもの、専門誌に掲載済みのもの、特許取得済みのもの、あるいは卒業論文など様々です。これらの様々な情報をその性質に合わせて適切に扱う必要があります。

■　様々な個人情報

大学には教職員の個人情報以外に、学生の個人情報や大学病院の患者の個人情報が保有されています。学生は毎年入れ替わるので大量の情報が蓄積されることになりますし、扱いがおろそかになる可能性もあります。また、患者の個人情報も日々蓄積されることになりますので、データは毎日更新しなくはなりません。また、患者の個人情報は重要な研究資源となりますので、研究者は自分の PC にインストールしたいという誘惑に駆られることでしょう。また、特定の患者を複数の医師が診るということになりますので、患者の個人情報はある程度オープンにする必要があります。

医師の PC にインストールされた患者の個人情報は大学内のネットワーク上に存在する場合に比して、その数倍、数十倍セキュリティ上の危険性が増していると言っていいでしょう。最近では PC 上に保存されている情報をコピーし

て転送してしまうようなウィルスも発見されています。

　個人情報は、個人情報保護法に抵触する問題をはらんでいるというだけでなく、情報が大量であれば、それだけで危険です。たとえば、ある特定の学部の学生の名前の情報が漏れれば、たとえその情報が名前の列挙だけだとしても危険性がないわけではありません。数百人の中には必ず、自分のアカウント名とパスワードを同じにしているなどという人間がいる可能性が高いからです。そのような人のうかつさが堤防を決壊させる蟻の一穴にならないともかぎりません。

第２章　セキュリティ上の脅威とその対策

2．１　セキュリティ上の脅威

セキュリティ上の脅威とその対策について理解するには、PC 等のデバイスの仕組みや、ネットワークとりわけインターネットなどの仕組みを理解していなくてはなりません。しかし、ここではそのような知識を前提としないで、できるだけ分かりやすく説明します。技術的な観点からいうと不十分な点もありますが、ご了解下さい。

セキュリティ事件の報道では、事件を起こした人物は通常ハッカーと呼ばれているようです。ハッカーという言葉は元々、コンピュータシステムに詳しい人という好意的な意味で使われますが、事件を起こした犯人が自分のことをハッカーであると自称することが多く、マスコミがそれをそのまま鵜呑みにしてしまったところから、悪いことをする人イコール「ハッカー」という定義が定着してしまったようです。ここでは、コンピュータシステムあるいはネットワークなどに対して攻撃をする人を「クラッカー」あるいは、「攻撃者」と呼ぶことにします。

２．１．１　外部からの脅威

外部からの脅威は様々ですが、ここでは簡単に不正侵入、ウィルス、DoS 攻撃について説明しておきます。

■　不正侵入

不正侵入とは、アクセスする権利のないシステムにアクセスする行為と言っていいでしょう。たとえば、他人の ID、パスワードを使ってシステムに入り込む行為です。通常、システムはアカウントとパスワードを与えられた人間だけがアクセスすることを許されます。従って、他人の ID とパスワードを使ってシステムに侵入する行為は当然許されません。クラッカーはどうやってパスワードを盗み出すのでしょうか。パスワードは、ゴミ箱に捨てられていたメモ用紙に書いてあったのかも知れません。ネットワーク管理者のふりをして言葉巧みに聞き出したのかも知れません。あるいは、デタラメにパスワードを入力したのかもしれません。大勢のユーザがいれば、ログイン名とパスワードを同じにしているユーザがいるものです。下手な鉄砲も数打ちゃ当たるです。手作業でこんなことをするのはいくら物好きのクラッカーでも大変です。しかし、インターネット上にはこのようなことを自動でやってくるフリーのツールがい

くらでも転がっています。最近はログイン名とパスワードが同じなどというのは、システムに拒否されますので、さすがにいないでしょうが、簡単に類推できてしまう安易はパスワードを使っているユーザは依然として多いはずです。

パスワードが分からなくてもシステムに侵入できる場合があります。たとえば、システムの開発者はシステムに入るのに一々セキュリティゲートをくぐり抜けるのはやっかいなので裏口を作っておくのが普通です。もちろん、システムが完成すれば裏口を閉じておかなくてはなりません。システム開発者がうっかり裏口(バックドア)を閉じておくのを忘れたら、その裏口はクラッカーの侵入口になります。あるいは、その裏口は他のクラッカーが自分で開けて、再度システムに侵入するときのために放置しておいたものかも知れません。

あるいはシステムの不具合(通常バグと言います)につけ込んで、システムに侵入することもあります。

システムに侵入したクラッカーが何をするかは奪取されたアクセス権のレベルと、侵入されたシステムの構成、クラッカーの技術力によって異なりますが、いったんクラッカーに侵入されたら後は、クラッカーのなすがままといっていいでしょう。

システムに侵入したクラッカーは、システムの不正利用をするかも知れません。不正利用するリソース(資源)はCPU、メモリ、ハードディスクなどです。ハードディスクが不適切なデータでいっぱいになっているかも知れません。あるいは、システムに不正なプログラムを仕掛けるかも知れません。この不正プログラムには様々なものがあります。たとえば、侵入されたシステムを足がかりにして他のシステムを攻撃するプログラムかも知れません。

あるいはネットワークを盗聴するという手を使うクラッカーもいるでしょう。データはネットワーク上をパケット(データの固まり)という形で流れます。そして、データの固まりの先頭部分(ヘッダといいます)には制御情報が記載されています。この制御情報を読み取るといろいろのことが分かります。ハブというネットワーク機器で接続されたPC同士の間を流れるデータは通信相手以外のユーザにも届いています。従って、もしデータが暗号化されていなければ、データの送り主と、その送り主のパスワードも分かります。もちろん、データの内容も分かってしまいます。しかも、そのようなことを可能にするフリーのプログラムが、インターネット上にごろごろと転がっていると思ってください。このようなツールはネットワークを管理するための有用なツールで、ネットワーク管理者にはなくてはならないものなのですが、これはクラッカーにとってもとても有効なツールです。

■　ウィルス

クラッカーによる不正侵入以上に質が悪いのがコンピュータウィルスです。コンピュータウィルスは、生身の人間に悪さをするウィルスと同様に、コンピュータに対して様々な悪さをします。

■　DoS 攻撃

DoS(Denial of Service)はいわゆる嫌がらせ行為です。この行為の結果、クラッカーが何かを得るというものではありません。他人が迷惑している様子を見て単純に喜ぶというたぐいの攻撃です。例えていうと、公道を我がもの顔で占拠している暴走族のようなものです。彼らはその行動で何らの利益を得ている訳ではありませんが、他人の利益/権利を侵害しています。つまり、自分で不当な利益を得ることではなく、他人を困らせて密かな喜びを得るという何とも始末に負えない攻撃です。基本的には DoS 攻撃には有効な対処法はありません。

２．１．２　内部の脅威

外部攻撃はインターネットを経由して外の世界からやってきます。外部からの攻撃は、様々なセキュリティの仕組みをかいくぐって内部ネットワークに到達して初めて可能になります。どんなにセキュリティが甘いネットワークでも内部に入るまでにはいくつかのハードルを越えなくてはなりません。外部からのシステム侵入者は、その苦労をいとわないと言っていいでしょう。しかし、内部者はハードルを越えるまでもなく内部ネットワークに接続しています。そして、内部ネットワークに接続していること自体で不審を買うということはありません。本来何らかのアクセス権限を持っているのですから、その権限を元にしてもっと高い権限を奪取することも可能です。また、内部者は内部ネットワークについて熟知している可能性も高いと言っていいでしょう。ネットワーク監視ツールを仕込んで、通信データを盗聴していても怪しまれないといった立場にもあります。あるいは、世間話の間にそれとなくパスワードなどの秘密情報を聞き出すことも可能です。つまり、内部関係者がひとたび悪事を行うつもりになった場合は、外部からの侵入者に比べて特段に有利な立場にいるということです。

２．２　セキュリティ事件が多発する大学

大学はセキュリティ事件の多発地帯と言っていいようです。しかも成功率も高いという統計的な結果も出ています。どうして大学ではセキュリティ事件が多発しているのでしょう。

■　インターネットは実験室であるという認識

インターネットは元々大学の研究者同士を結びつけるもので、様々なネットワーク実験を行うためのプロジェクトであったと言っていいでしょう。今日のように、インターネットが一般に開放されても、大学人には「インターネットは自分たちのもの」、一般の人にはただ「間借りを許しているだけ」だという意識があるのではないでしょうか。しかし、もうその考え方は許されません。一般の商用利用者も、大学のユーザも対等の立場でインターネットに参加しなくてはなりません。

■　サーバ管理は片手間の仕事であるという認識

大学の関係者にはサーバの管理程度のことは専門の仕事ではない、ボランティアが研究の合間に片手間の仕事としてこなす程度のもの、あるいは学生のアルバイトで十分こなすことのできる簡単な仕事という認識があるのではないでしょうか。しかし、サーバの管理はそんなに簡単なことではありません(もちろん難しいというほどのものでもありませんが)、ただ動けばいいというのとよく管理されているのとでは天と地ほどの差があります。

■　インターネットはオープンな世界であるという認識

インターネットに参加するデバイスは、IP アドレスを割り振られています。そして、リモートのネットワークデバイスと通信したい場合は、どのネットワークに存在するどのホスト(デバイス)上のどのアプリケーションというように相手を指定します。どのネットワークに存在するどのホストというように指定する場合の識別子が IP アドレスと言われる番号です。つまり、IP アドレスはどのネットワークという識別子と当該ネットワーク上のどのホストという識別子が一緒になっているというわけです。どのアプリケーションかを識別するのがポート番号と呼ばれる数字です。

IP アドレスにはグローバル IP アドレスとプライベート IP アドレスがあります。グローバル IP アドレスは外部ネットワークとの通信を許された IP アドレスです。プライベート IP アドレスは自由に使用することができますが、外部

ネットワークとの通信を行うためには特別な仕掛けが必要です。プライベートIPアドレスを使っているネットワークは外部ネットワークからは見えません。通常は、外部から内部に接続しようとしても不可能です。これに対してグローバルIPアドレスは外部に対して公開しているIPアドレスと言っていいでしょう。外部から内部ネットワークが丸見え状態です。外部から内部ネットワークに接続することが可能です。

一般的な企業では外部に対して公開すべきネットワークのみにグローバルIPアドレスを割り当てます。通常外部に対して公開すべきものとは、メールサーバとWebサーバ、DNSサーバだけです。このような公開サーバを設置するネットワークは通常、DMZ(非武装地帯)ネットワークといい、そこに設置するサーバには特別なセキュリティ上の配慮が必要です。それ以外のサーバやPCはファイアウォールの背後の内部ネットワークに隠しておきます。そして、内部ネットワークにはプライベートなIPアドレスを割り振ります。

大学のネットワークはどうでしょうか。大学のネットワークは通常、すべてのデバイスにグローバルIPアドレスが割り振られています。そして、内部ネットワークはファイアウォールで防御しているのですが、内部ネットワークにもグローバルIPアドレスが振られていますので内部は透け透け状態です。

インターネット上のシステムはクライアントサーバシステムという仕組みを利用しています。これは、クライアントから能動的にサーバに対して働きかけて通信を行う方式です。内部ネットワークにはサーバが存在しないなら、クライアントサーバシステムを前提とする限り、内部ネットワークが透け透け状態でもそれほど気にする必要はありません。しかし、内部ネットワーク上のPCにサーバをインストールすることは簡単です。内部ネットワークが透け透け状態で、つまり内部ネットワークにグローバルIPアドレスが割り当てられ、そこにサーバが起動しているなら、外部ネットワークから内部ネットワークに対して接続を確立することが可能です。もちろん内部ネットワークと接続するためにはファイアウォールなどのセキュリティシステムをかいくぐらなくてはなりませんので、簡単とは言えませんが、クラッカーの触手を刺激することは確かでしょう。

大学では実に様々なホームページが立ち上がっています。社会に対して開かれた大学としては沢山のホームページが起動している状態はいいことに違いありません。しかしたとえばある学科に在籍する学生の名前だけを掲示するホームページにどれほどの意味があるのか疑問です。このようなものは大学のセキュリティを危うくするだけで何の意味もないと考えます。社会に対して開かれた大学を標榜するためには、必要な情報は公開しなくてはなりません。しかし、それは意味もなく情報を公開して、大学のセキュリティを危うくすることが許されるということを意味しないはずです。情報を公開する際には、セキュリティが危うくなることがないように最大限の防御策を講じる必要があるということです。

２．３　セキュリティ対策の必要性

ここまで説明すると何でセキュリティが必要なのだという読者はいないと思いますが、とりあえず大学でセキュリティ対策を行う必要性についてまとめておきましょう。

■　社会の一員としての責務

大学も、社会に存在する組織の一つですので、社会的組織が守るべき最低限の規範には従わざるを得ません。そして、大学を構成するメンバーも社会の一員ですので、当然社会人としての責務があります。不正侵入をしてはならないというのは当然のことです。そのほかに踏み台にならないこと、ウィルスを巻き散らかさないようすることなどです。踏み台になるというのは、クラッカーが群馬大学のネットワークに侵入し、群馬大学のネットワークを経由して他の組織を攻撃するような場合を指します。この場合、群馬大学は積極的には何も悪いことをしていません。しかし、踏み台になるようなシステムをそのまま放置していたという消極的な関与をしています。踏み台を使うとあたかも、その踏み台の被害に遭ったシステムが外見上、攻撃者であるかのように見えます。メールサーバや、Web サーバ、ルータ(主要なネットワーク機器です)などでは、どのようなシステムからアクセスがあったかなどをログという仕組みで保存しています。このログの記録上、踏み台から攻撃されたように一見すると見えると言うことです。つまり、クラッカーは踏み台を見つけると、それを隠れ蓑にして悪いことができるのではないかと勘違いしてしまいます。これは犯罪行為を誘発する行為、刑法で言えば犯罪の教唆、あるいは幇助に当たると言ってもいいかも知れません。

ウィルスにかかった本人は、そのことに気づかずにウィルスをまき散らしてしまうこともあります。しかし、今日のようにウィルスが猛威をふるっている時代には、常に自分がウィルスに罹っていないか注意することが社会的責務として求められます。

■　大学のブランドを守る

大学のブランドを守るということは、あの大学は教育をしっかりしている、卒業生が優秀で活躍している人が多い、いい研究が行われている、などという評判を維持することです。これからは、あの大学は情報セキュリティがしっかりしているなどということも大学のブランド力の１つになるでしょう。

これからは、企業と大学との共同研究なども盛んになることが予想されます。

そのような時に、あの大学と共同研究すると情報が漏れてしまうなどという評判を立てられてしまったら大変です。

■　個人情報保護法への対策

個人情報保護法は 2005 年の 4 月から施行されています。個人情報保護法が本格的に施行されるようになると「知らなかった」では済まされません。違反すれば、文科省やマスコミから責め立てられ大学の評判は傷つけられることになります。

■　訴訟問題に巻き込まれないために

システムやネットワークへの攻撃に、大学のサーバが踏み台として利用されたということになると訴訟問題に巻き込まれることもあり得ます。踏み台に使われると、表面上はその大学から攻撃が行われたように見えます。このような場合でも、大学のシステムは単に踏み台として利用されただけで何らの過失もないということを証明できなくてはなりません。そのためには適切にログを管理し、クラッカーに足下をすくわれないように日頃の備えをしておく必要があります。踏み台として利用されたシステムの管理が不十分ならば、管理不十分なままのホストを放置し不正な行為を誘発したということで、責任を問われる可能性もあります。つまり、やるべきことをやらなかったという不作為の罪ということです。

クラッカーはログを書き換えるなどということもやり兼ねません。こうなると、ログを解析しても単に踏み台として利用されただけでなく、その大学が攻撃の発信元であると判断される可能性があります。ログを書き換えたら、ログを書き換えたこと自体がログに残っていなくてはなりません。

ログを解析した結果、濡れ衣を免れたとしても、踏み台として利用された大学の評判は大いに傷つけられる結果になります。

２．４　セキュリティ対策

ここでは代表的なセキュリティ対策について説明します。

２．４．１　ネットワーク構成の見直し

群馬大学に特徴的なこととして分散キャンパスという事情があります。この分散キャンパス間をいかに安全に接続するかが課題になります。このような分散キャンパスを安全に接続する技術としてはVPN(Virtual Private Network)という仕組みがあります。公衆網を使いながら、専用線接続と同様のセキュリティを確保する技術です。

グローバルIPアドレスとプライベートIPアドレスの話は既にしましたが、本当にセキュリティが必要なネットワークはプライベートアドレスを使い、外に出て行くときはNAT(Network Address Translator、ネットワークアドレス変換)という仕組みを使うべきです。NATの中側は外からは見えない状態になるので、外側からNATの内側に向けて接続を張ることは殆どできません。

２．４．２　認証システム

認証システムとは、システムを利用する権利があるか、サービスの利用者／提供者が信頼できるかなどをチェックする仕掛けです。皆さんに一番なじみ深いのがパスワード認証でしょう。

その他にはIDカードを利用した認証システムや、生物学的特徴を元に認証を行うバイオメトリックス(Biometrics)などがあります。IDカードを使った認証には、IDカードを紛失したり、奪われたりしたときにどうなるのかという問題があります。バイオメトリックスを使えば、紛失したり奪われたりという問題は起こりませんが、システムそのものがまだ完全でないという問題があります。たとえば、声紋を利用する声紋認証では風邪を引いたりして声が変わったりした場合に認証が行えない場合があります。最近、精度が高く使いやすいということで実装が増えているのが手のひらや指先の静脈の形を元にした認証システムです。

また、電子署名というシステムもあります。これはPKI(Public Key Infrastructure 公開鍵基盤)という暗号化を用いた認証システムを使って、電子署名された文章に、現実世界の実印を押された文章と同様の公的証明力を付与する仕組みです。

２．４．３　暗号化

データの盗聴、書き換えなどに対処するためには暗号化技術を使います。暗号化はアプリケーションレベルでデータの中身だけ暗号化する場合から、通信路自体を暗号化してしまう方法まで様々な方法があります。通信の内容だけ暗号化する場合は、誰と誰がどんなアプリケーションを使ってデータのやり取りをしているかは分かりますが、その通信の内容は分かりません。通信路自体を暗号化する方法にも様々な方法があります。通信をするもの同士の間では、パケットというデータの固まりがやり取りされますが、通信路の暗号化ではデータの固まりの先頭部分にある制御情報(この部分を通常ヘッダといいます)まで、ひっくるめて暗号化されますので、誰と誰とがどんなアプリケーションを使って通信をしているかということまで分からなくなります。従って、通信路そのものを暗号化してしまった方がより安全と言うことになります。ただし、通信路を暗号化する場合は、データそのものの暗号化に比べて大仕掛けになるので、コスト面や使い勝手の面で大変です。

２．４．４　アンチウィルス

コンピュータウィルスは、コンピュータの中でよくない動作をするプログラムです。一概にウィルスといっても様々なものがあります。どのようなプログラムをウィルスというかは一応定義はされています。また、広い意味でのウィルス、狭い意味でのウィルス云々などという言い方もあります。しかし、今日は細かい話はやめておきます。

ウィルスが厄介がられるのは殆どのウィルスが電子メールの添付ファイルに感染する形でやってきたり、インターネットからのダウンロードという形でやってくることです。電子メールの添付ファイルに感染してやってくるかも知れないので「今日から電子メールは使わないことにしましょう」、ということでコンセンサスが得られる組織ならば、セキュリティを確保することも簡単でしょう。また、インターネットからダウンロードするプログラムは危険なので、今日からインターネットからはダウンロードしないことにしましょう。こちらはどうでしょうか？こちらは比較的コンセンサスを得やすいかも知れません。しかし、Web を使っていると知らないうちに危ないプログラムをダウンロードしてしまう可能性があるので、「今日から Web は使用禁止」と言われたらどうでしょうか。電子メールも使わない、Web も使わない、これではインターネットに繋いでいる意味がありません。もちろん、セキュリティが最優先のネットワークでは、こうせざるを得ないでしょうが、組織全体にこれを認めさせることはできません。特に大学などでは研究活動が成り立たなくなります。

ウィルスは大部分メールに添付されてやってきますので、メールが必ず通るところにアンチウィルス(ウィルスチェッカー)をおいておけば、ウィルスをブ

ロックできます。メールが必ず通るところ、それはメールサーバと呼ばれるシステムです。メールサーバが稼働しているマシン(コンピュータ、通常ホストと呼んでいます)をメールサーバということもあります。

ただし、問題は大学では多くのメールサーバが稼働しているということです。どのメールサーバでアンチウィルスを動かしておけばいいのかという問題があります。インターネット上のプログラムはフリーのものが多く、しかもフリーのソフトの方が優れているということが珍しくありません。しかし、アンチウィルスは例外です。コンピュータウィルスは型を持っています。これはA ソ連型とか、A ホンコン型とか、B 型とかいったインフルエンザの型と同じです。そして、型にぴったり合うかどうかという検査(マッチング)を行います。アンチウィルスソフトは従来発見されているウィルスのデータベース(通常、定義ファイルといいます)と、ウィルスと疑われるプログラムとのマッチングを行い、型が一致すれば、そのプログラムをウィルスと判定します。コンピュータウィルスは毎日のように新型が作られていますので、定義ファイルもその都度新しいものに更新していかなくてはなりません。世の中には良心的なプログラマーは沢山いますが、この作業を毎日ボランティアでやってくれる人はさすがにいないようです。従って、アンチウィルスは市販のソフトメーカのプログラムを使わざるを得ません。

アンチウィルスソフトは、定義ファイルに記述されたものをウィルスと認定しますので、できたてのウィルスはチェックできないという問題もあります。

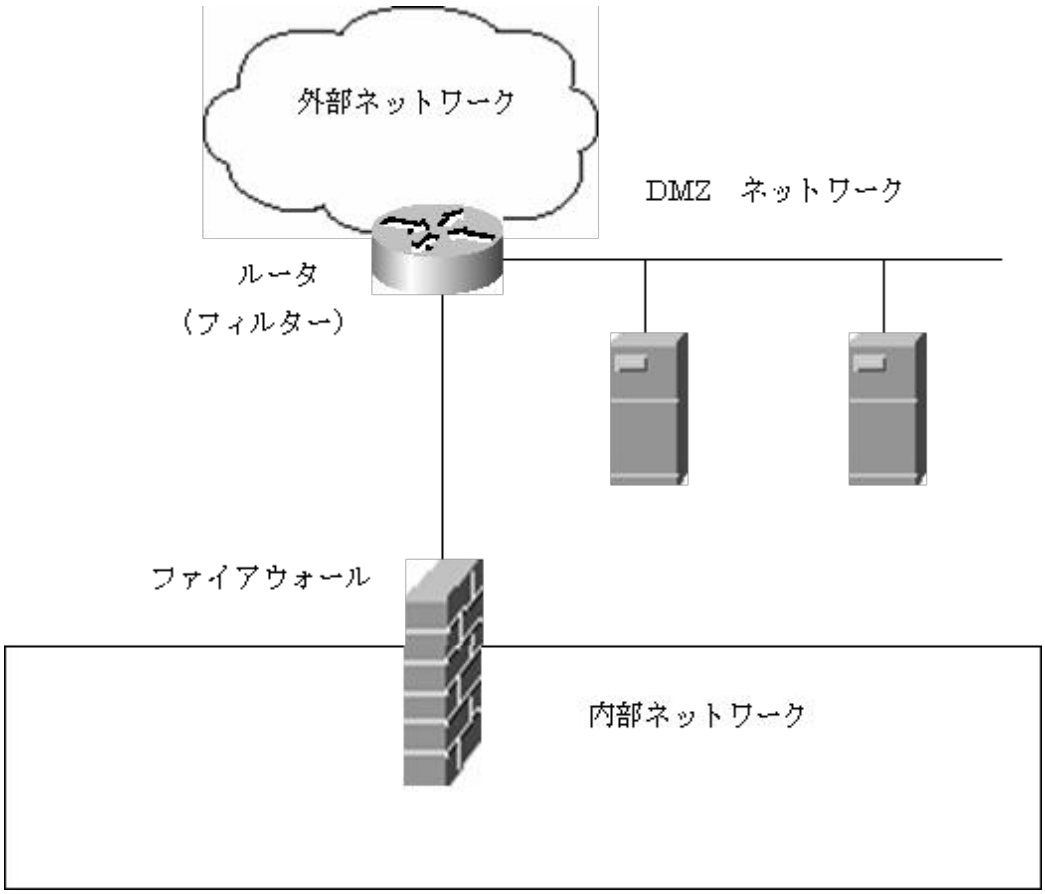
アンチウィルスがどんな定義ファイルを使っているか、つまり何をもってウィルスと認定するかの根拠は、当然各ソフトメーカの企業秘密です。従って、あるメーカがウィルスと認定しているプログラムを、他のメーカのアンチウィルスはウィルスでないと判定する可能性もあります。従って、いろんなメーカのアンチウィルスを使った方がいいわけですが、コストの問題がありますので、通常は特定のメーカのソフトをメールサーバに入れたら、他のメーカのソフトは各ユーザのパソコンに入れるということになります。

更に問題があります。大学で使用するパソコンは守れたとしても、家で使用するパソコンはどうするかという問題です。家で罹ったウィルスを大学に持ち込むという場合もありえます。学生が家で使うパソコンにも、大学の費用でアンチウィルスソフトを入れるというのは理想ですが、大学でそこまで面倒を見ることはおそらくできないでしょう。

２．４．５　ファイアウォール

ファイウォールは一頃情報セキュリティを守るための伝家の宝刀のように言われたことがあります。何年か前のお正月に通商産業省(今の経済産業省)のホームページが中国のサーバ経由で侵入したクラッカーによって書き換えられるという事件が起きました。この事件の報道では、「ファイアウォールが設置

されていなかったもよう」などというコメントが一緒に流されました。これなどは、ファイアウォールさえ設置しておけば侵入されなかったのかもという誤解を一般の人に与えました。何でこんなコメントが流されたのかは分かりません。たぶんその当時はセキュリティの専門家などはまだ存在していなかったのではないでしょうか。マスコミがたまたまコメントを求めたネットワークの専門家がファイアウォールを余りよく理解していなかった結果だと思います。そもそも、一般に公開しているホームページというものは、外部からアクセス可能なネットワーク(グローバル IP アドレスを割り振られています)に設置されたホスト上に置いておきます。誰でもアクセス可能な状態にしておかなければなりませんので、ファイアウォールで守るということはできません。外からいつでもアクセスできる状態にしておく必要があるのは、メールサーバなども同じです。組織のメインのメールサーバは、外のネットワークからいつでも接続できる状態になっていなくてはなりません。そうでなくては、外からのメールを受け取ることができません。



ファイアウォールは、内部にあるホストを外部ネットワークからの不正な攻撃から守ることが目的です。しかし、常に外部ネットワークとの接続を保証しなくてはならないメインのメールサーバや公開の Web サーバ、組織を代表する DNS サーバなどはファイアウオールの外側に置いておく必要があります。これらのネットワークは弱肉強食のインターネットの世界と、内部ネットワークを分離するネットワークですので通常、非武装地帯(DMZ、DeMilitarized Zone)などと呼ばれます。DMZ に設置したサーバはそもそもファイアウォールでは守ることができないということになります。上の図では、ルータ上でフィルターという仕掛けが稼働しています。このフィルターも広い意味ではファイアウォールですが、そもそも公開サーバが置かれている DMZ の外側に置かれているものですから、それほど強い規制をかけないのが普通です(公開サーバをどれくらい公開するのかというレベルの問題になります)。

ファイアウォールは、外部ネットワークと内部ネットワークの境界線上に設置して、サービスをブロックするか、通過させるかという判断をして内部ネットワークを守ります。メールはいったんメールサーバで受け取ったものを各ユーザが自分のパソコン上にダウンロードしますが、そもそもファイアウォールでメールをブロックすることはできません(メールを使わないというコンセンサスが得られれば別ですが)ので、ウィルスをブロックすることはできません。Web サーバはそもそもファイアウォールの外側に設置されていますので、当然ファイアウォールで守るというのは論外です。

こう考えるとファイアウォールは案外非力であるということが分かると思います。もちろんなくてもいいというものではないのですが、伝家の宝刀などでは決してないことは分かっていただけると思います。ただし、市販のものでファイアウォールと言われているものは、次に説明する IDS(侵入検知システム)やネットワーク管理システムなども一緒になっているものが多いのでそれなりに強力になっています。

２．４．６　侵入検知システム

侵入検知システムは通常 IDS(Intrusion Detection System)と呼ばれます。IDS にはネットワーク型の IDS(NIDS、Network IDS)とホスト型 IDS(HIDS、Host IDS)があります。

ネットワーク型の IDS はネットワークを流れるパケットの内容を元に情報収集を行います。侵入や攻撃で使われるパケットはある程度の規則性を持っていますので、IDS はこれらの規則性をデータベースとして持ち、ネットワークに流れるパケットが持っている規則性とマッチングをして侵入や攻撃の検知を行います。予め登録しておいたデータベースにマッチしないと検知はできません。このような方式は通常、不正検知と呼ばれます。不正検知では新手の攻撃を見つけることはできません。しかし、侵入行為や攻撃は正常な行為とは違った特

徴を持っているはずです。このような性質は、異常と言っていいでしょう。統計的に見て普段の状況とは違うということで異常を発見する方法を異常検知といいます。異常検知を使うと未知の攻撃を発見することができますが、攻撃ではないものを攻撃とミスジャッジする可能性もあります。

ホスト型の IDS は IDS を仕込んだホストに対する侵入・攻撃だけを検知します。様々なアプリケーションは、そのシステムに対するアクセスをログとして残しています。ホスト IDS は、そのログファイルをモニタリングして、侵入・攻撃を検知します。また、システムの完全性をチェックする仕組みを利用するような方法もあります。システムのインストール時の侵入や攻撃にまだ遭っていないまっさらな状態の時に、システム(ファイル)の指紋(finger print)を採っておきます。その後定期的に、システムファイルを指紋と比較することで整合性のチェックを行い、侵入・攻撃を検知する手法です。

２．４．７　手に負えない厄介者

情報セキュリティを守るためには様々な技術がありますが、ここまでその中の代表的なものを説明しました。しかし、これだけやっていれば大丈夫という決め手なるような仕掛けはありません。しかも、やっかいなことに今まで説明した対策が余り役に立たないような攻撃が最近多くなっています。

■　DoS 攻撃

DoS 攻撃とは、Denial of Service(サービスの拒否)攻撃という意味です。DoS 攻撃がやっかいなのは DoS 攻撃を仕掛けるクラッカーが何も求めていないことです。彼らの目的は正規のユーザがシステムやネットワークを利用するのを妨げるだけです。つまり、正規ユーザが困っているのを遠くから傍観して、密かに喜んでいるような輩です。

アクセス権を奪うのはなかなか大変です。いくつかの関門をくぐり抜けてやっとアクセス権限のないシステムに侵入することができます。いくつかの関門をくぐり抜ける時に、クラッカーの行為はその都度記録(ログといいます)に残ります。しかし、アクセス権を奪う訳ではないとすると関門は極めて少数です。あるいは関門がないかもしてません。これではクラッカーの行為が記録として残りません。つまり、攻撃者が誰なのか記録に残らない訳です。攻撃者の立場からすると、足跡の残らない攻撃、あるいは指紋の残らない攻撃ということになります。

アクセス権を奪うわけではないので技術的に遙かに簡単です。殆ど技術力のないものにも使える DoS 攻撃用のツールがインターネット上には無数に転がっています。

DoＳ攻撃には様々な形態のものがあります。そのうち代表的なものを２つ紹介しておきます。１つは俗にメール爆弾と呼ばれるタイプです。電子メールは、メールサーバの間を転送されます。メールサーバは郵便局のような働きをします。エラーメールを受け取ったメールサーバは、メールのヘッダに記載された返信先アドレスあるいはエラーの通知先アドレスにエラーが発生したことを知らせます。もし、返信先アドレスあるいはエラー通知先アドレスを偽造した(攻撃対象のアドレスに書き換えます)エラーメールが大量に発送されると、エラーの通知が一度に攻撃対象のサーバに到達して、そのサーバは、処理が追いつかずにダウンしてしまいます。

２つ目の例はSYN Floodなどと呼ばれます。ヘッダの特定部分(SYNという名前のフィールド)のビットが立っているパケットが大量に送られてきて、その処理が間に合わなくなったシステムはダウンしてしまいます。インターネットのプロトコルであるTCP/IPには、コネクション型の接続と、コネクションを確立しない接続があります。通常ユーザがよく使うアプリケーションはコネクションを確立してから通信を行います。このようにした方が信頼性の高い通信ができるからです。コネクションを張るというのは、相手を素性を確認して納得してから通信を始めるということです。インターネットでは通常、クライアントサーバシステムという仕組みで通信を行います。アクティブに接続を確立するのは必ずクライアントです。サーバは、パッシブにクライアントの要求に応じて接続を開始します。例えていえば、クライアントがサーバさんのお宅に伺いこれこれのことをしたいと要望を出すようなものです。サーバさんのお宅に伺ったクライアントは玄関に通されます。サーバさんが納得すれば、応接間に通してもらえます。応接間に通されると、クライアントの相手をするサーバさん宅の使用人がいて、クライアントの頼み事を聞いてくれます。ところが、玄関でサーバさんが納得して、中へどうぞといったのにクライアントが玄関にとどまっているとしたらどうでしょうか。また、クライアントが玄関に入ってきました。このクライアントは実はグルなのです。また、中へどうぞと言われたのの玄関に居座ります。続いて、またまた仲間のクライアントがやってきて玄関に居座ります。こうすると、どんな大邸宅でもすぐに玄関が一杯になってしまいます。どうしてでしょう。玄関は最初に挨拶する際に使用するだけで、その後中に通されるという前提でできていますので、どの家でも余り広くはないのです。玄関が一杯になると新しいクライアントが入ってくることができなくなります。つまり、新しい接続は確立できないことになります。これが代表的なDoS攻撃であるSYN Flood攻撃です。クライアントサーバ型のコネクション接続では、3ウエイハンドシェークという手順を踏んで挨拶を行い、相手の素性を確認します。クライアントがサーバさんの大邸宅の玄関に入り挨拶をする動作が１つ目の動作、次にサーバさんがどうぞ中へお入りなさいというのが2つめです。そのサーバさんの言葉に応じてクライアントが中に入るのが3つめの動作です。この３つの動作を一まとめにして、3ウエイハンドシェークといいます。クライアントが最初にサーバさんのお宅に伺って玄関に入って挨拶する動作と、サーバさんが中へどうぞという言葉を発する動作は、パケットで

言えば両方ともヘッダのSYN(ビット)フィールドという部分に1がセットされています。つまり、SYN Food攻撃はSYNビットがセットされたパケットを大量にサーバに送りこむ攻撃ということになります。

SYNパケットを送るという行為そのものはTCP/IPの手順に沿った行為で何ら攻撃的なことではありません。しかし、その後に続いて行われるべき行動を故意に行わないということによって不都合な結果を招いています。エラーメールを送るという行為も、それ自体は別段なんら悪いことではありません。悪いことをしようという意識がなくてもエラーメールを送ってしまうことはしばしばあるでしょう。つまり、DoS行為は個々の行為を表面的に判断すると、迷惑行為なのかどうかが判断できないのです。しかし、それが悪意を持って大量に行われると大変な迷惑行為になります。個々の行為を表面的に判断すると、迷惑行為なのかどうかが判断できないということは、DoS攻撃をブロックするツールは作りにくいと言うことになります。

さらにやっかいなことにDoSはウィルスなどと組み合わされて使われることが多いと言うことです。ウィルスに感染したシステムが同時多発的に特定のターゲットを攻撃するなどという場合もあります。このようなDoS攻撃は通常DDoS(分散DoS、Distributed DoS)などと呼ばれます。DDoSはDoSよりも遙かに質の悪い攻撃となります。

■　P2P

P2P(Peer to Peer)のPeerとは英語では同じ階層の仲間という意味です。身分制度の残っている英国では、同じ貴族同士ということになります。Peer to Peerですから、同じ身分のもの同士の通信です。これはクライアントサーバシステムと対立する概念です。インターネットは一部の例外を除いてその殆どがクライアントサーバ型のシステムです。当然のことながらインターネットのセキュリティシステムもクライアントサーバ型のシステムをいかにセキュアに運用するかという前提でできています。したがって、P2Pのアプリケーションはセキュリティを考える上では大問題ということになります。

P2Pは、不特定多数の個人間で直接情報をやり取りするインターネットの利用形態で、多数のコンピュータを相互に接続して、ファイルや演算能力などのリソースを共有するシステムです。P2Pの利用形態は大きく分けて2つに分類されます。１つは、中央サーバを使うタイプです。サーバはファイル検索サービスや、ユーザ間の接続管理を提供しますが、ユーザ同士のデータ交換等はユーザ間で直接行います。もう１つは中央サーバを使わずにバケツリレーをするタイプです。このタイプは全部ユーザ間で直接行います。サーバが介在している場合は、そこに監視プログラムを置いておくことで違法データの交換など

を効率的に発見することができますが、サーバが介在しないということになると当局が規制をするという観点からは、極めて対処の難しい相手ということになります。現実には、最近サーバを使わないP2Pプログラムが多くなり、著作権法違反や違法データの交換などの問題を起こしています。

■　コンテンツの不適切な公開

コンテンツを不適切に公開するこも問題です。ここでは、一つの例として匿名 Remailer について説明しておきます。今まで何度もヘッダの話をしました。メールの場合も例外ではありません。TCP/IP(インターネットのプロトコル、プロトコルとは通信の手順、つまり約束事のことです)に代表されるパケット型の通信では、パケットの先頭部分(ヘッダ)に制御情報が記述されています。メールの場合では誰が発信したメールであるかなどの様々な情報が記述されています。誰が発信したメールであるかはFrom:フィールドというところに書かれます。たとえば、匿名のメールでもヘッダ部分を解析すれば、どこのホストから発信されたメールか分かります。どのホストから発信されたメールかが分かれば、メールの差出人もだいたい分かるでしょう。しかし、匿名 Remailer という仕掛けは、特定のメールアドレスにメールを送信すると、From:フィールドの内容等を書き換えて、個人情報が特定できない形でメールの転送やニュースへの投稿を行います。このような仕掛けが簡単に利用できるようになると根拠のない無責任な誹謗中傷が盛んにおこなわれるようなことになりかねません。

第3章　セキュリティマネジメント

今回の講演の趣旨は、「従来、ネットワーク管理者が一人で頑張っていれば、組織のセキュリティはどうにか維持できたが、もう限界に来ているということ」、「組織の情報セキュリティを維持するためには情報セキュリティをマネジメントしなくてはならない時代に突入したということ」を分かってもらうことです。したがって、セキュリティをマネジメントするということがどういうことなのかまでは、詳しく説明する余裕はありません。

ということで、実際の講演(30分)ではセキュリティマネジメントについては殆どさわり程度しか話すことができませんでした。しかし、このまま終わってしまうのはいかにも尻切れトンボですので、情報セキュリティマネジメントの概略だけ、講演の後で書き足しました。従って、この後は殆どの部分が講演の後で書き足したものです。

■　情報セキュリティマネジメントシステムとは

情報セキュリティマネジメントシステムは通常、ISMSと呼ばれています。ISMSとは、情報を適切に管理し、機密を守るための包括的な枠組みです。コンピュータシステムや、ネットワークのセキュリティ対策だけでなく情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用についてのトータルなマネジメント体系をひっくるめて情報セキュリティマネジメントシステムといいます。

３．１　情報セキュリティとは

情報セキュリティを考える場合に、ポイントになるのは機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)です。これらは情報のCIAと呼ばれますが、情報セキュリティとは、このCIAを如何にして守っていくかということです。

更にGMITS(ISO/IEC 13335)は、次の3項目を追加しています。GMITSの3項目は、説明責任制(Accountability)、認証性(Authenticity)、信頼性(Reliability)の3つです。

３．１．１　情報のCIA

■　機密性(Confidentiality)

情報の機密性とは、ある情報をどの程度の厳格さで秘密扱いするかということです。情報の読み込み、書き込み、実行などが正規のユーザの権限に従って適切に管理されているならば機密性が高いということになります。

■　完全性(Integrity)
　完全性とは、データが正確かどうかということです。データが正確ということは、データの内容が正確ということと、データ作成者の作ったままの状態で後で権限のない第３者に改ざんされていないということを意味します。

■　可用性(Availability)
　可用性とは、必要な時に確実にアクセスできることです。

３．１．２　GMITS の３項目

■　説明責任性(Accountability)
　何かセキュリティ事件が起きたときに、実際に何が起きたのかを説明できることです。実際には、ファイアウォールやサーバ、ルータなどへのアクセスログを記録することの必要性と言っていいでしょう。

■　認証性(Authenticity)
　認証性とは情報にアクセスしてきた者が本物であることを認証することです。

■　信頼性(Reliability)
　信頼性とは入力されたデータと出力されたデータの整合性を取ることです。

３．２　セキュリティポリシー

　情報の CIA と GMITS の３項目を守るためには、守るべき項目を文書化し、組織全体に知らしめなくてはなりません。この「文書化された規約」がセキュリティポリシーです。

３．２．１　セキュリティ規約の階層化

　セキュリティポリシーは作り放しで、後は神棚に奉っておくだけというのではセキュリティは向上しません。セキュリティポリシーを作ったらそれを実行しなくてはなりません。セキュリティポリシーには決まった書き方というものはありませんが、法律体系でいえば、憲法に当たるもの、法律に当たるもの、省令あるいは規則に当たるものを作っていきます。これは通常、基本ポリシー、スタンダード、プロシージャなどといわれます。基本ポリシーが憲法に当たるものですから、いろいろな場合に対応できるようにある程度抽象化しておく必要があります。スタンダードは、基本ポリシーの宣言に基づき、実際に基本ポリシーを実践する基準を作ります。スタンダードは組織内の実際の運用に沿って検討する必要があります。最後に部署ごとに、各部門の担当者が守るべき基準をプロシージャ(実施手順書)として作成します。手順書は実際に適用する手

順が書かれたものですから、頻繁に変更する必要が出てきます。しかし、変更はスタンダードの範囲内にかぎられます。

３．２．２　リスク分析

セキュリティポリシーの策定過程では、リスク(危険)分析が非常に大きな比重を占めます。リスクを分析するためには、まずリスクを構成する要素について知る必要があります。

■　リスクを構成する要素

リスクを構成する要素は情報資産と、脅威と、脆弱性です。情報資産とは、その組織の活動等を支援する有形／無形の要素の中で、それが失われたり損なわれたりしたら、その組織に損失が発生するもののことです。脅威とは、情報資産に直接／間接的に損失を与える要因となるものです。脆弱性とは、損失を発生させ、拡大させる要因となるものです。

■　リスクの分析

リスクの分析では、情報資産の洗い出し、脅威の洗い出し、脆弱性の洗い出しを行い、しかる後に人の分析、リスクの分析と評価を行い、最後に対策を策定します。

●　資産の洗い出し

情報資産とは、たとえば経営情報や顧客情報などです。この情報資産は紙の形かあるいはデジタル化されているのか、どこに保存されているのか。紙ならば誰が、どこに、何枚保存しているのか、社内に回覧される場合はあるのか等、デジタルデータならば、どのホストに保存されているか、そのホストのセキュリティレベルはどの程度か、アクセス権はどうなっているのか、暗号化されているのか、メールに添付されることはあるのか、バックアップはどうか等が検討されなくてはなりません。これらの情報資産の機密性、完全性、可用性を点数化し、情報価値を判定します(たとえば１億円の資産価値というように)。

●　脅威の洗い出し

①　脅威を起こす主体となるのはだれか、クラッカーなのか社員なのか、クラッカーはおもしろ半分の愉快犯か、それともプロフェッショナルか。脅威を起こす主体によって脅威のレベルが違ってくるはずです。

②　脅威を起こす主体は、何を目的としているのか。いたずらか、金銭か、それともテロか。いたずら目的ならば、DoS 攻撃や、ホームページに改ざん程度で済むかも知れませんが、テロが目的ならば社会的なインフラを破壊していく可能性があります。

③　脅威はいつどのような形で発生するのかも考慮しておく必要があります。サービスのピーク時かそれとも夜中か。頻度も問題です。毎日攻撃される場合と、1 年に 1 回程度では脅威のレベルが違ってきます。

④　どのような攻撃方法が使われるか、技術的な面の検討も必要です。外部からインターネットを通じて行われる攻撃と、部内者によってサーバに対して直接行われる攻撃では脅威のレベルが違ってきます。

以上の①～④の観点から脅威の内容を洗い出します。たとえば、「主体：クラッカー、目的：いたずら、時間：1 年に 1 度、手法：ネットワークダウン、脅威の内容：サービス停止」のように特定していきます。

●　脆弱性の洗い出し

脆弱性の洗い出しは、まず脆弱性の対象となるものをリストアップし、その対象のどこに問題があるのか、どのような状態が問題なのかを分析します。
脆弱性の対象になるのは、脅威の原因になるもので、「人」、「物」、「組織体制」など様々です。
たとえば、脆弱性の対象に Web サーバを選んだ場合は、問題と状況は、「OS のバージョンが古い」、「Web サーバソフトのバージョンが古い」、「Web サーバソフトの設定基準が守られていない」などということになります。

●　人の分析

人の分析とは、たとえば、属性(大学でいえば教員、非常勤教員、事務職員、学生、大学病院の医師、看護師等)、職種、技術力、所在(殆ど学内にいる人と

頻繁に電車で移動したり、喫茶店に立ち寄る人では脅威の度合いが違います)、精神(大学に対して不満を持っている人かどうか)や、肉体の状態(健康体かどうか)、勤務状態(何日も徹夜作業をやっている人は注意力が散漫になっているかも知れません)、IT の知識・経験などの着眼点を持って分析することです。

● リスクの分析と評価

リスクの分析と評価とは、情報資産の洗い出し、脅威の洗い出し、脆弱性の洗い出し、人の分析を行った結果をそれぞれ関連づける作業を行い、損失の発生する可能性を分析し、発生の確率を算定することです。

関連づけ作業を行うことで、どのようなリスクが存在し、その重要度はどの程度なのかをハッキリさせます。関連をハッキリさせるためには枝葉末節な事柄は思い切って切り捨てる現実的な対応が必要になります。診断チェックリストを用意するなどの工夫が必要です。

損失発生の可能性を正確に算定するのは無理ですので、組織内で過去に発生した問題の履歴、組織内でのアンケート調査、最近の政府機関の調査結果、マスコミの報道などを元に算出します。ただし、既に何らかのセキュリティ対策が施されている場合は、そのことによって問題発生の確率は減少しているはずですので、その点も考慮に入れる必要があります。

リスクが顕在化した場合の損失額は次の計算式を使って算出することができます。

（直接損失 ＋ 間接損失 ＋ 対応費用）× 損失発生の確率

● 対策の策定

対策の策定は、リスク自体に対して行う方法と、脆弱性に対して行う方法が考えられますが、脆弱性に対して対策を考えた方がすっきりします。１つの対策で複数の脆弱性に対応できる場合が多いからです。

脆弱性に着目して、対策を策定する場合の手順は次の通りです。

① 脆弱性に着目して、対策を洗い出す。

② 対策の観点から脆弱性をグループ化する

③ 洗い出された対策とリスクを関連づける

対策とリスクを関連づけることで、対策のリスクに対する効果が見えやすくなります。

対策は主にリスクコントロールと、リスクファイナンスという形で行います。リスクコントロールとは、リスクに対して物理的、技術的、管理的対策を行うことです。リスクファイナンスとは、リスク損失が発生した場合に、復旧にかかる対応費用や損失の補填にかかる費用を確保しておくことです。準備金、積立金を用意するとか、情報セキュリティ保険に加入するなどの方法が考えられます。

３．２．３　ポリシーの作成と運用

ここでは、情報セキュリティポリシーを作成して、運用するまでの全体的な話をしたいと思います。

■　組織作り

情報セキュリティポリシーを策定するためには、そのセキュリティポリシーをどこに適用するのかを決めます。大学全体に適用するのか、大学病院に限定して適用するのかなどで、セキュリティポリシーを推進するための組織の構成員も異なってきますし、当然のことながらセキュリティポリシーも違ってくるはずです。

適用範囲が決まったら次にセキュリティポリシー策定のための実働部隊を集める必要があります。実働部隊のメンバーは、そのセキュリティポリシーが実際に適用されることになる範囲の組織から横断的に集めます。情報セキュリティポリシーは実際に適用しなくては意味のないものですので、組織の実情にマッチしていなくてはなりません。そのためには組織の業務の現状をよく知っている担当者を集める必要があります。また、セキュリティポリシーができたらそれをトップダウンの形で適用する必要がありますので、それにふさわしい人がその組織のリーダーでなくてはなりません。

■　スケジュール

スケジュールを決めないと動き出さないのが人の組織の常ですので、スケジュールを決めます。情報セキュリティポリシーは一般的には３ヶ月～6 ヶ月位の期間で作成します。あまり長くなりすぎますとリスク分析が組織の実情に合わなくなり、結果として出来上がったポリシーが適用には不適切になってしまう可能性があるからです。最初は３ヶ月程度でセキュリティポリシーを作り上げるのは難しいかも知れませんので、ひな形を参考にするのがいいでしょう。

■　リスク分析

リスクを分析するためにははじめに組織の現状を調査する必要があります。調査の方法としては、ツールを使ってサーバ等の脆弱性を調査したり、セキュリティベンダーが提供する「侵入検査サービス」などを使って実際に侵入できるかどうか調べるやり方などがあります。

次に、各業務の詳細を把握している担当者からのヒアリングなどを通して、業務の流れを洗い出し、その業務の中でどのような情報が扱われているか、その情報のなかで「情報資産」となるものはなにか、その情報資産に介在している「人」は誰なのかを洗い出していきます。リスク分析に詳細については既に説明しましたので省略します。

■　情報セキュリティポリシーの作成

リスクの分析ができれば、組織の中で「守るべき情報資産は何か」がハッキリしてきます。守るべき情報資産がハッキリすればあとは、それを守るための方針を明確にして文書化し、それを組織の構成員に伝えることが重要になります。その文書化された方針が情報セキュリティポリシーということになります。

セキュリティポリシーは、基本セキュリティポリシー、スタンダード、プロシージャという形で文書化するのが普通です。

基本ポリシーは情報セキュリティ体系の憲法に当たるものですから、できるだけ抽象化して記述します。執行部からの宣言が含まれ、執行部の情報セキュリティに対する基本姿勢が示され、組織の構成員に対して遵守を促すものとなりますので、通常は宣言文の形になります。

基本ポリシーはスタンダードで敷衍します。スタンダードは、組織内の業務運用の実態に合わせたものでなくてはなりません。

プロシージャは、部門や担当者ごとに守るべき手順書になりますので、実態に合わせて頻繁に改訂する必要があります。

■　情報セキュリティポリシーの運用

基本ポリシー、スタンダード、プロシージャが作成できたら、大学の執行部から承認を得なくてはなりません。執行部からのお墨付きがあって初めて情報セキュリティポリシーは組織の全構成員に対して強制力を持った「指示書」となることができます。組織の全構成員に対して強制力を持った「指示書」は、組織の全構成員の前に公開し、それに従うことを求めることができます。

公開するセキュリティポリシーは常に最新のものであることを保証するために、バージョンと変更履歴の管理をしっかりしなくてはなりません。また、作成された文書の存在と内容は周知徹底させることが必要です。また、プロシー

ジャが実際に適用されていることを、内部監査やシステム監査等で確認していくことが大切です。

３．３　セキュリティ標準と認定制度

情報セキュリティポリシーは各組織の業務実態に合わせて設定されますので、当然のことながら組織ごとに違ったものになります。しかし、政府機関や外国企業と取引を行う場合などには情報セキュリティポリシーが整備されているかどうかが一つの物差しとして使われる場合があります。物差しとして使われるということになると、各組織が勝手に決めればいいというわけにもいきません。そこで、「ものさし」として使うのならば、何らかの基準を満たしているべきだということになります。この場合に使われるのが「標準」といわれるものです。

代表的な「標準」はISO/IECが標準化したISO/IEC 15408と、ISO/IEC TR 13335(GMITS)、英国規格協会が定めたBS7799です。

ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) 15408は情報処理システムや情報関連製品が、それぞれどのようなレベルにあるかを評価するための標準です。この標準はJISに取り入れられてJIS X 5070として規格化されています。

BS 7799は、BSI(British Standards Institution)によって発行された情報セキュリティマネジメントに関する仕様を記述した規格です。BS 7799はパート１とパート２から構成されます。パート１は、網羅的な実践規範で、パート２は英国内での実装をにらんだ補足条項です。パート１は、ISO/IECの標準に取り入れられてISO/IEC 17799なっています。

ISO/IEC TR 13335は一般にはGMITS(Guidelines for the Management of IT Security)と呼ばれます。GMITSは、IT(Information Technology)とセキュリティ(Security)を管理するためのガイドラインです。

日本では、ISO/IEC 17799とGMITSを加味したものをJIS X 5080として発行しています。

以上が代表的な標準です。いずれも情報セキュリティマネジメント(ISMS、Information Security Management System)する場合に守るべき基準を提供します。しかし、基準に沿ったいくら立派な仕組みを作ってもそれが実際に実行されていない場合は絵に描いた餅ということになります。そこで、基準がしっかり守られているかを評価し、認定する制度が必要になります。これが、ISMS

適合性評価制度と呼ばれるものです。ISMS 適合性評価制度では、第 3 者である審査機関が ISMS 認証基準(現在は Ver2.0)に照らして認証を希望する組織の適合性を判断します。