情報セキュリティ技術向上研修を受講して

宇　野　智　則*
uno_to@jim.kit.ac.jp

1990年代にインターネットが普及するまで、コンピュータウィルスは主にフロッピーディスクなどを介して感染することがほとんどで、それも画面の文字が崩れ落ちていくとか、画面にメッセージを表示するとかといったいたずら目的の物ばかりでした（中にはハードディスクのデータを消去するような悪質な物もありましたが…）。

インターネットの普及に伴い、ネットショッピングやオンラインバンキングといったサービスも現れ、それらの情報を盗み取ることを目的としたサイバー犯罪が増えてきました。更には政府機関を標的とした攻撃や、病院のシステムを麻痺させて患者を人質に金銭を要求するような攻撃も現れています。そしてもちろん大学も攻撃の例外ではありません。

しかしながら、自分達のシステムがサイバー攻撃に対して万全なのか、どこか弱いところがあるのかといったことは気づきにくく、また地震に遭うまでその備えの大切さに気づかないのと同じように、被害に遭うまでつい対策を怠ってしまいがちなもので、実際に攻撃に遭う体験のできる研修というものはとても重要なものです。

9月6日～7日に名古屋大学で開催された文部科学省主催の「情報セキュリティ技術向上研修」では、一人でサーバ構築・運用をやっていた担当者が1週間海外旅行に行くので後を任され、今まで何事もなかったのが奇跡のような状態のサーバ群に次々と攻撃が襲い来るという、実際には絶対に体験したくない設定で始まりました。

参加者は3人一組でチームを組み、インターネットに見立てた仮想のネットワーク環境に、各チームのネットワーク内に置かれたウェブサーバやメールサーバなどのサーバが接続され、競技運営者が攻撃を仕掛けて来ます。

本来ならば、まだとても外部に公開できるような状態にないのですが、サービスをできるだけ停止させずに適切な設定を加えていくよう要求されており、会場前方には各チームのサーバの状態が表示されます。何事もなければ緑で表示され、サービスにアクセスできなくなれば赤くなります。我がチームは（チームメイトの情報科学センター秋山さんと春田さんのお陰で）一度も赤くなることなく済んだのですが、次々と赤くなっていく様は恐ろしいものでした。

名称	OS	主な動作ソフトウェア	主な通信要件
FW	CentOS 6	iptables	-
Web1	CentOS 6	Apache, PHP, mysql	HTTP(80/tcp), HTTPS(443/tcp)
Web2	Windows Server 2008 R2	IIS	HTTP(80/tcp), HTTPS(443/tcp)
DNS/NTP	CentOS 6	bind, ntpd	DNS(53/tcp, 53/udp), NTP(123/udp)
Mail	CentOS 6	postfix, dovecot	SMTP(25/tcp), IMAP(143/tcp)
Proxy	CentOS 6	squid	PROXY(8080/tcp)
NAS/Log	CentOS 6	samba, rsyslog	CIFS(445/tcp), syslog(514/tcp)

図1 防御対象のシステム

サーバを外部の攻撃から守る一番の方法は外部との接続の一切を遮断することですが、もちろんそれではサーバの意味がなく、必要な通信を許可しつつ、不要な通信は全て許可しないようにしなければなりません。必要な通信まで不許可にしてしまうと忽ちサーバの状態は赤くなります。赤くなっている間でも次の攻撃は容赦なく始まり、ほとんど何もできずに終わってしまったチームもあったようです。

研修では多くの設定をLinuxのコマンドラインで行う必要があり、日頃グラフィカルインターフェースしか使わない人には厳しかったと思いますが、GUIが使えないような場面に直面することも充分に考えられるので、システム

＊情報管理課情報企画係長

管理者であれば使えるようでなければなぁと感じさせられましたが、特に事務職員にとってはなかなか習得できる機会もなく、このような研修の前に必要な知識の習得が課題であると感じました。

そしてシステムで対策を取ることが難しく、昨今被害が拡大している攻撃が標的型攻撃で、これは実際の業務のメールを模した文面で送られてくるために一見して攻撃だと気づきにくく、被害に遭いやすい攻撃です。こればかりは現状ではシステム管理者だけで対策するのは困難なので、全学的に標的型攻撃メールの模擬訓練を行うなどの訓練が必要だと感じました。

怒濤の攻撃をしのいで初日が終わり、二日目はどのような攻撃が行われていたのか解説が行われ、初日になんだか分からない内にやられてしまった攻撃についても理解し、対策を知ることができました。

サイバー攻撃は受けてからもたもたしているとあっという間に被害が甚大なものになります。本研修を通していかに早く攻撃を察知し、分析し、対応策を講じるかがとても重要であると改めて実感しました。そのためには日頃から迅速な対応が取れるよう連絡体制を築いておく必要があります。

またCMSなどでユーザーに管理を任せているものは、なかなかしっかりとアップデートを実施できているか把握しきれず、システムの脅威になり得ることも実感しましたが、各管理者に確実に対策をしてもらえるようにすることは難しく、今後の課題だと思いました。

丸二日かけた研修でしたが、実践型の研修で得られるものは多かったと思います。是非今後も多くの人に本研修を受講してもらえるようお勧めしたいです。また研修で使用した環境を構築するのはコストもそれほどかからないと思いますので、自分の機関で構築して訓練できるように広まることも期待したいです。