ネットワークセキュリティに対する提言

総合情報処理センター　鳩野逸生

1. はじめに

昨今，インターネット環境において，ブロードバンド化が急速に進んでいる．つい数年前まで，一般家庭からのインターネット接続は，せいぜい 50kbps のダイアルアップ接続が大多数だったものが，昨年から，一挙に 1.5Mbps, 8Mbps の ADSL, 100Mbps の FTTH(Fiber To The Home) が低コストで導入可能になって来ている．すでに一人あたりのインターネット接続回線容量でいえば，神戸大学より家庭の方が大きい，といった現象も起こっている．その中で，政府による電子政府の取り組みや，電子商取引の拡大などが予想を上回る速度で進展する一方，多くの問題が生じてきているのも確かである．その中の主要な問題の一つが “ネットワークセキュリティ” である．本稿では，神戸大学におけるネットワークセキュリティの過去，現在について述べるとともに，総合情報処理センター内で議論されている今後の神戸大学のネットワークセキュリティの提言について述べる．

2. 神戸大学におけるネットワークセキュリティ

神戸大学のネットワーク運用を議論する「情報ネットワーク運用委員会」の議事録に,「ネットワークの不正アクセスについて」という項目が現れるのは，平成 9 年 12 月に開催された委員会からである．それには，某部局で不正侵入があり，パスワード漏洩の恐れがある，と記されている．それ以来，委員会が開かれるたびに欠かされることのない話題になっている.「ネットワークの不正利用」として報告される事項としては，以下のものがあげられる．

(1) 第三者による不正利用
  (a) メールの第三者不正中継
  (b) DNS, Web サーバ等のセキュリティホールからの侵入およびパスワードの不正取得, 盗聴, 他計算機への不正侵入
(2) 内部からの不正利用
  (a) AUP(Access User Policy), ネットワーク利用規程に反する利用

この他に，ネットワークの不正利用の範疇に直接は入らないが，コンピュータウイルス (worm) への感染が，ネットワークセキュリティに関して重要な問題の一つとしてあげられる．

2.1 神戸大学の現状

神戸大学において，平成 9 年から 11 年頃にかけては，(1)-(a), (1)-(b) に関しての報告がほとんどであったが，平成 11 年より，コンピュータウイルスの中で，自己を増殖するために，ウイルス付きのメールを自動的に感染した PC から発信するとと

もに，(1)-(b) も同時に行う機能を持ったものが出現した．典型的な例として，Code Red[1] があげられる．Code Red は，感染すると，他の Web サーバを攻撃し，成功すると，その Web サーバの内容を書き換える．また，Nimda といわれる worm はさらに悪質で，感染するとウイルス付きメールはばらまく，Web サーバは攻撃する，等々多くの手段で増殖を試みるため感染力は非常に高い．２つの worm は，平成 12 年の夏から秋にかけて世界的に大流行し，大きな被害が発生した．神戸大学内でも多くの PC, Web サーバが被害にあった．総合情報処理センターでは, 被害を最小限にするため，SINET と神戸大学の間で, Web アクセスを監視し，worm からのアクセスがあればフィルタリングする，という措置をとった[1]．その時点で，外部からの全 Web アクセスの 40~50%が両 worm からのものであったことを観測している[2]．この種の複合的な機能を持ったウイルス, worm の大きな問題点は，感染した PC, Web サーバのみならず，ネットワークに大きな負荷をかける，という点である．これはうわさで信憑性は不確実であるが，Code red, Nimda が大流行している時点では，某プロバイダの海外向け回線のトラヒックのほとんどが両 worm からのものであった，という報告もある．現在も，www-admin@kobe-u.ac.jp 宛にくるメールの 30~40%はウイルス付きメールであり，爆発的な流行こそ無いものの，予断を許さない状況であると思われる．

2.2 現状のセキュリティ対策

結論から先に述べると，セキュリティ対策は各部局，学科に一任しているというのが現状であろう．部局によっては Firewall やウイルススキャン機能を持ったメールサーバを独自に導入しているところが存在する．事務部門では，ウイルススキャンソフトウエアのライセンスを大量に取得し，導入している PC へのインストールを義務づけている．総合情報処理センターの計算機システムでは，Firewall を導入するとともに，すべての Windows 系 PC にウイルススキャンソフトを導入している．しかし，大学内の多くは，無防備なところが多いものと推測される．そのような状況を少しでも改善するため，KHAN2001 導入後，前述の通り，総合情報処理センターでは，KHAN から SINET への出口で，ウイルスによる Web アクセスのフィルタリング, セキュリティホールがあると報告されているサーバが利用する通信ポートで, 通常学外からアクセスする必要がない，と思われるものを閉じるている.[3] これらの設備は，KHAN2001 に関連して導入したものである．Firewall システムの構成を図 1 に示す．この他，KHAN2001 導入時に，各部局に設置した Layer 3 スイッチ[4]で，各部局申告によるフィルタリングを実施している. また，事務部門の，ATM 網を利用したプライベート・ネットワークへの隔離を実行した．この他，各部局で独自にサーバを管理運用する手間を削減するため，総合情報処理センターで，レンタル DNS サーバ, www.kobe-u.ac.jp サーバの学部，学科への解放を進めている[5]．また，総合情報処理センターでは，ユーザの管理を軽減するため，Radius サーバ, Samba を利用し

[1] 10 月 ~12 月間を除き，現在も継続中である．
[2] 現在でも，外部からもっとも多いアクセスは, ウイルスまたは worm からと思われる．
[3] セキュリティ上の見地からすべてを公表することはできない．鍵をかけている窓とかけていないドアを公衆に公開することを考えればご理解いただけるかと思う．
[4] IP ルーティング機能を持つスイッチのこと．KHAN2001 では基幹スイッチと呼んでいる．
[5] 詳しくは，総合情報処理センター業務掛へお問い合わせください．

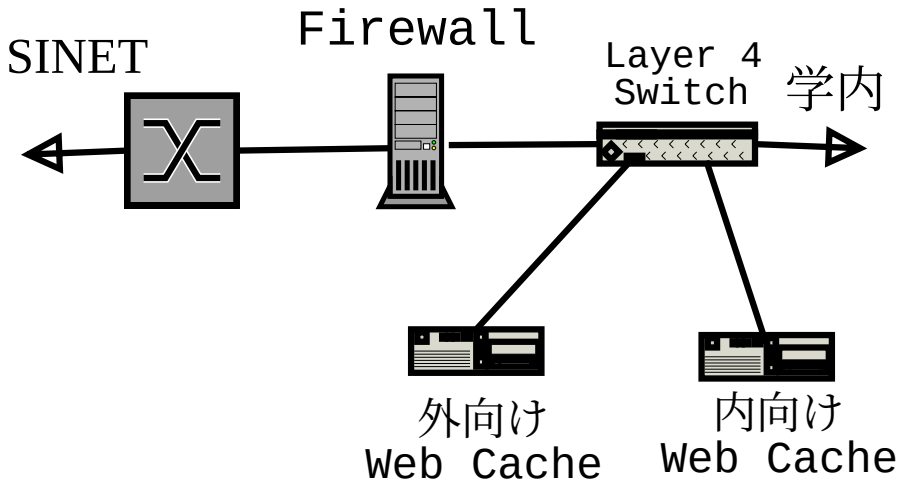

Fig. 1: 神戸大学 Firewall システムの構成

た Windows 端末認証サーバを準備している．各部局等で自由利用を前提とした端末を導入する場合は，センターに是非ご相談いただきたい．

現状で一番問題な点は，

- 部局，学科によりセキュリティに対する意識，対策にばらつきが大きい．何も対策していないところもあると推測されるのに対し，過剰反応としか思われない処置をしているところもあること．
- 全学的にも（おそらく各部局単位でも）セキュリティ対策に対するポリシー（セキュリティポリシー）が存在しない[6]．

ということであろう．後者の問題は，特に全学的にセキュリティ対策を浸透させる当たって非常に重要かつ必要不可欠であるが，全学的な合意のもとで作成，運用する必要がある．セキュリティ意識が薄い人は，多くの場合以下のような反応を示す．

- (セキュリティ対策の不備を指摘されて) セキュリティを守ることは大事だが，学外から自分のサーバからデータが取れないと困る．
- (同上) セキュリティ対策を取る時間がない，セキュリティ対策のために時間が取られる．
- （例えばあるサーバにアクセス制限をかけた場合）勝手に使い勝手を悪くすると困る．

いうまでもないが，セキュリティー問題を考えるあたっては，セキュリティー対策を実行したことによる不利益（利便性の喪失）と万一重大情報の漏洩等が発生したときの被害の大きさを比較する必要があるが，重大な事故が発生する確率はかなり低いため，セキュリティー問題に対する十分な情報が与えられない場合，意思決定にはかなりのばらつきが発生する．

神戸大学に限らず大学には，学生の学籍情報，成績情報などの個人情報，あるい

[6] もし作成されている部局があれば情報管理室までお知らせいただきたい．

は共同研究などにおける秘密を要する情報[7]が, 数多くインターネットからアクセスできる計算機上に存在していると思われるが，幸いにして大きな流失事件は発生していない.

2.3 外部の動向

一般には，現在，各組織毎に適切なセキュリティポリシーを定め，実行するということは常識になってきている．google 等の検索エンジンで，セキュリティポリシーというキーワードで検索すると，数多くのセキュリティポリシーの策定，運用のコンサルタントに関するページがヒットすることからもお分かり頂けると思われる．

しかし，国立大学に関していえば，かなり遅れた状況にある．現時点で，セキュリティポリシーを制定している大学はまだ少数であると思われる．一昨年の省庁ホームページの大規模クラック事件を契機に，政府機関におけるセキュリティポリシーの策定，実行が進められているが，その一環として国立大学においてもセキュリティポリシーを策定し，実行せよ，との要請が文部科学省から来ている．現在，事務系，研究・教育系におけるセキュリティポリシーの雛形を作成中である，とのことである．

近隣の大学に目を向けると，京都大学でその一端を見ることができる．京都大学は，昨年度の補正予算で措置されたネットワーク構築において,「セキュリティ確保」を主要な目的に据えている．詳しいことは，京都大学の KUINS のページ [2] をご参照いただくとして，割り当てアドレスはすべてプライベート, 固定アドレスは原則として割り当てず，すべて DHCP[8]，デフォルトではセグメント外に通信不可で必要なところだけに許可する，など徹底している．また，大阪大学においても，原則として，学外から直接学内の計算機にアクセスできなくする，といった対策をとる，と聞き及んでいる.

3. 神戸大学におけるネットワークセキュリティポリシー策定に向けて

前述の状況を鑑みると，神戸大学においてもセキュリティポリシーを作成し，抜本的なセキュリティ対策を講じる必要があると思われる. これまで神戸大学で取ってきた,「各部局，利用者に任せる」という方法では，対処することはもう困難であろう. また，万一現在の状況を継続し，大きな問題を引き起こした時，十分なセキュリティ対策を取っていなかった，ということで引きおきした問題以上の影響が及ぶものと予想される[9].

セキュリティポリシーを決めるには，まず「守る対象」を決定および分類し，そのそれぞれについて「どのように守るのか」を考察する必要がある. 大学において守るべき情報は，以下のようなものになると思われる.

学生の個人情報: 学籍（成績）情報, 健康診断情報など

職員の個人情報:

職員全般: 給与，保険, 勤怠，人事考課など

連絡先: 所属，電話，FAX, E-mail アドレスなど

研究/教育資料・資源・成果

[7] 特許出願を予定している情報など．これから独立行政法人化に伴い，増加するものと思われる.
[8] IP の動的割り当て機構の一種
[9] 特に，ネットワーク関連の予算獲得に影響が出ると思われる.

授業資料: プリント, 板書原稿, OHP シートなど
研究内部資料: 実験データ, 研究ノート，内部ミーティング資料など
研究公開資料: Web 上, 論文ファイル, 学会発表資料など
教官業績: 職歴, 発表論文，受賞歴など

学生，職員の個人情報に関しては，連絡先を除けば原則的に非公開にすべきものであるが，研究/教育資料・資源・成果に関しては，公開してもいいものとそうでないものに関してきちんと管理する必要があり，十分な考察が必要である. 逆に言えば，研究/教育資料・資源・成果を学内ネットワーク上に接続された計算機上で管理する場合，公開/非公開のコントロールが適切に行われている必要がある. ご存知の通り，インターネット上では日々新しいセキュリティホールをついたクラックツール, コンピュータウイルス/worm などが発生しており，それらにきちんと対処することは大変な労力を要する[10] これを個々の利用者に要求することは非現実的であると考えられる．むしろ，Firewall の設定を, 原則的に対外公開は禁止するように設定し，少数のきちんと管理されたサーバのみ対外公開するように方針を変更することが現実的であると考える.

また，今までは外部からの不正進入のみを考えていたが，内部の人員が不正（または事故で) に情報をリークしたり，破壊活動をすることも考慮する必要がある. これは，学内ネットワークにつながる計算機およびその利用者を管理する必要があるということを意味する. もし，つなぎさえすれば誰でも利用できるようなポートや誰でもユーザ認証なしに利用できる計算機が存在した場合，いくら入り口で制限してもそれ自体が大きなセキュリティホールとなる． 内部利用者の利便性を落とさないためには，学内に接続された計算機からの利用制限を緩める必要があるためである.

また，学生の個人情報の事故による流失を防ぐには，セキュリティが甘く設定されている教官の計算機にそのような情報を蓄えることを制限することが必要になるであろう. また，学生のみならず教職員に対しても情報セキュリティーに関する講習受講[11]を義務づけるということも必要である.

これに関して，京都大学での例のように，徹底的にネットワーク側で管理する，という方法もあるが，最終的には, 各部局・利用者にご協力頂くしかないであろうと思われる.

4. おわりに

本稿では，神戸大学の周辺を中心としてネットワークセキュリティの状況について述べるとともに，セキュリティポリシー策定における問題点について述べた. 前述したように，本省から雛形が届き次第，具体的な作成に入るということになるかと思われるが，是非全学的な視野からのご意見を頂ければと思う.

参考文献

[1] http://www.cert.org/advisories/CA-2001-19.html
[2] http://www.kuins.kyoto-u.ac.jp/

[10] 特に Microsoft 社製品の場合. 個人的には対外公開用サーバとしては勧められない. むしろ禁止すべきではないかと考えている (ただし，禁止の実行は困難である).
[11] または試験