ネットワークグループ活動報告 2001

— ネットワークセキュリティに関する活動報告 —

山本好弘（工学部技術部 第2技術系第4班）　新美治利（工学部技術部 第1技術系第1班）

1．はじめに

現在、工学部技術部ネットワークグループの活動の一つとしてネットワークサーバ（以下、サーバと称す）やクライアントパソコン（以下、パソコンと称す）をはじめとする情報機器の管理・運用がある。[1)]これらの情報機器は通常の業務や学生に対するサービスを行う上で重要であり、特にメールサーバやネームサーバなどのネットワークサーバは停止することはできない。従って、各サーバを常時稼動できるように、不意な停電からサーバを保護するための無停電電源装置(UPS)の導入、故障に対する備えとしての定期的なデータのバックアップ及びバックアップ用サーバの準備をしている。

現在、インターネット上で多くの商用、公共サービスが行われるようになり、様々な人々が簡単にインターネットに参加（アクセス）出来るような環境が整って来たこともあり、インターネット人口の急速な増大と共に、ネットワーク関連の犯罪（悪戯）も増加してきている。それに伴い、ネットワーク（インターネット）を支える各種サーバはクラッカーと呼ばれる攻撃者の対象となり、安全に常時稼動させるには彼らクラッカーからサーバを守るためのネットワークセキュリティが重要視されるようになって来ている。

今回の報告では、ネットワークグループで通常行われている情報機器の管理方法をネットワークセキュリティを中心として紹介するとともに、大学内にて多数のサーバが感染・発症したコンピュータウイルス(Nimda)への対応と駆除の実例を併せて報告する。

2．情報機器の管理業務

ここでは、現在ネットワークグループにて行っている主な情報機器の管理業務を紹介する。特に注意を払っているサーバのセキュリティ関連を中心として、日常どのような管理を行っているかを述べる。

2.1 管理下にある情報機器（サーバ、パソコン）

ネットワークグループで管理を行っている主な情報機器とその管理形態を以下に示す（表1）。また、管理形態は情報機器によって異なり、ネットワークグループによる直接管理と事務部からの依頼によって行う間接管理の形態がある。

表1　管理を行っている主な情報機器

所　属	情 報 機 器	管理方式
工学部	Webサーバ	直接管理
工学部事務部	メール・ネームサーバ	直接管理
	パソコン（多数）	間接管理
就職情報室	ファイアウォール	直接管理
	パソコン（8台）	

注）各サーバ、ファイアウォールは各1台

2.2 サーバの常時稼動の必要性とその対策

現在、情報発信としてのWebサーバ、メールの送受信を行うメールサーバ及びインターネット接続を可能にするネームサーバが常時稼動し、その中でも特にメール、ネームサーバは業務を行う上で必要不可欠なものとなっている。また、学生の就職活動、勉学を支援するために設立された就職情報室のサービスも重要な位置を占めており、何れのサーバも長時間停止することは出来ない。

次にサーバ停止の主な要因とそれに対する対

策を示す（図１）。

○落雷等による不意の停電が起こるとハードディスクがダメージを受ける効能性がある。これにより、ファイルシステムの破壊等が引き起こされ、データの損失やサーバの起動が出来なくなるなどの被害が予想される。これに対しては、無停電電源装置(UPS)を導入することにより、不意の停電に対しサーバが安全に停止するための時間の確保を行い、ファイルシステムの破損等を防ぐことができる。

○ハードウェアの故障等によるサーバの停止及びそれに伴うデータの損失（ファイルシステムの破壊、ハードディスクの障害等）に対しては、バックアップサーバの準備と定期的なデータのバックアップによる迅速な復旧を行えるようにしている。

○クラッカーからの攻撃（以下、クラッキングと称す）によるサーバのサービス停止、ファイルの破壊及び他サーバ等への攻撃の踏み台への利用に対するセキュリティ対策として、ログの監視、セキュリティホールへのパッチ当て及び各種サービスへのアクセス制限などを行っている。また、クラッキング行為にはコンピュータウイルス（以下、ウイルスと称す）を使用したものもあり、ウイルスの感染・発症及び拡散を防ぐためのセキュリティ対策はサーバだけでなく、パソコンに対しても行っている。

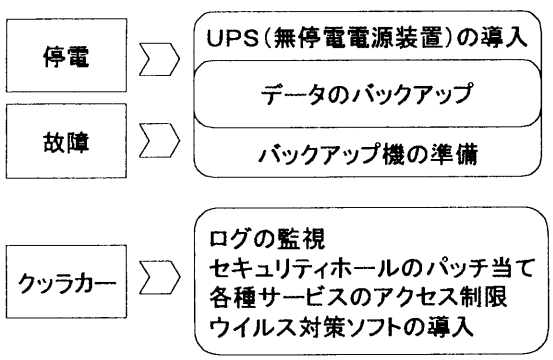

図１　主な障害の要因と対策

2.3 ネットワークセキュリティ[2)]

先に述べたように、サーバ停止の主な要因として停電、故障及びクッラキングが考えられるが、この要因の中で停電及び故障に関してはある程度有効な対策が取られている。しかしながらクラッキングに対する有効な手段は無く、常に様々な対策を行って行かなければならない。また、クッラキングはサーバだけでなくパソコンに対しても行われており、十分な対策を行う必要がある。ここでは、ネットワークセキュリティの必要性やネットワークグループで行っている、サーバ及びパソコンに対するクッラキング対策の概要などを紹介する。

2.3.1 ネットワークセキュリティの必要性

ネットワーク（インターネット）に接続されている情報機器（特にサーバ、パソコン）は、常にクラッカーの攻撃対象となる危険がある。以前の研究機関同士による情報共有としてのネットワーク利用とは異なり、現在のネットワークはインターネットの商用利用を始めとして様々な利用が行われている。それに伴って様々な人々がネットワーク（インターネット）を利用するようになり、ネットワーク世界にも悪戯や犯罪を行う人達（クラッカーなど）も増加してきている。特に常時稼動し、インターネット上で各種サービスを提供しているサーバは攻撃の目標となる。

以下にクラッキングをはじめとする様々な攻撃によって引き起こされる主な被害を示す。

○サービスの中断・停止

DoS 攻撃によるサーバへの過負荷、ウイルスの侵入・発症によるファイルの破壊及びクラッキングによるサーバの機能停止による提供するサービスが中断・停止することによる被害。

○データの漏洩・破壊

ウイルスの侵入・発症及びクラッキングなどにより、サーバ上のデータを盗まれたり破壊されたりする被害。企業のサーバであれば機密情報、

顧客リスト及び管理者 ID・パスワード等、個人のパソコンであればメールやユーザ ID・パスワードなどが盗まれる可能性がある。

○社会的信用の失墜

クラッキング又はウイルスの侵入・発症等により、

・ホームページの改竄等による反社会的メッセージの発信

・アカウント等の不正使用による“なりすまし”

・SPAM と呼ばれる迷惑メールの中継を行う

・ウイルスの発信元となる

などの事態を引き起こす可能性がある。

なお、社会的信用の失墜による被害は自分自身から見れば被害を受けたようにも思えるが、その際のサーバなどからの発信による被害を受けた人から見れば加害者となる。また、第三者からのクラッキング等が行われた事を証明できたとしても、充分なセキュリティ対策等を行っていなかった場合は、管理不十分として何らかの責任を追及される事にもなりかねない。

また、ウイルスによっては感染・発症後に自分自身を添付したメールを自動発信するなどの行為を行うものもある。この様なウイルスによる他者への攻撃は、サーバのみならずパソコンでも起こるので注意が必要となる。

2.3.2 セキュリティの考え方

ネットワークグループで直接管理している各サーバ及びパソコンがクラッキング等により受ける被害を想定し、それに対する基本的なセキュリティの方針を示す。

①者還元奪取の防止

攻撃への踏み台となることの防止

ホームページの改竄の防止

②ウイルスの拡散に対する防止

③データの損失及び流出の防止

④各種ネットワークサービス停止の防止

なお、各サーバ、パソコンは提供しているネットワークサービスや用途が異なるので、個々の特徴やそれに対する対応は以下に述べる。

○工学部 Web サーバ

・工学部のオフィシャルな情報をホームページにて発信。

現在、情報の発信のみで、掲示板等の開設や在学生に対する Web によるサービス等は行っていないので、短期間の停止では大きな問題とはならない。また、サーバ内には特に重要な情報も存在しない。

・セキュリティの方針

ホームページの改竄等による反社会的なメッセージの発信及びクラッカーによる攻撃の踏み台となることを防ぐことを第一とする。

○事務部ネーム・メールサーバ

・事務棟に所属する（席のある）職員のネームサービス（ネットワーク接続）やメールの送配信を行う。

メールサービスの停止は様々な業務を行う上での障害となるので常時稼働させる必要がある。

・セキュリティの方針

クラッカーによる攻撃の踏み台及び SPAM（迷惑）メールの中継に利用されることなどを防ぐことを第一とする。また、メールサービスを利用したウイルスの拡散防止及びメール内容の喪失、漏洩に注意する必要がある。

○就職情報室ファイアウォール（サーバ）

・就職情報室のパソコンをグローバルのネットワークから切り離す。

現在、通過するサービスは http のみであるので、ローカル側のパソコンの用途はインターネットによる情報収集及び Web メールの送受新端末程度であるが、就職活動等における緊急性を要するメールの送受信なども想定されるので常時稼働を目標とする。

・セキュリティの方針

クッラカーによる踏み台となる事を防止するのが第一とする。また、ローカル側からグローバル側への悪戯防止も考える。

○就職情報室パソコン

・インターネットによる就職情報の収集及びWebメールの送受信端末。

・セキュリティの方針

ホームページの閲覧、ファイルのダウンロード及びメール添付ファイル等によるウイルスの感染・発症を防ぐことを第一とする。パソコンはファイアウォールにてグローバルのネットワークから切り離されているのでネットワーク経由でのウイルス拡散の可能性は低いが、フロッピーディスクによるオフラインでの拡散の可能性があるので注意する必要がある。

2.3.3 セキュリティ対策

上記のセキュリティの考えに基づき、実際のセキュリティ対策を紹介する。なお、セキュリティの問題上詳しく述べることができないので、概要のみに留めておく。

各サーバのセキュリティ対策として

・セキュリティホールを塞ぐ

・ログの監視

・各種サービスのアクセス制限

などを常時行っている。

また、パソコンのセキュリティ対策としては

・セキュリティホールを塞ぐ

・ウイルス対策ソフトの導入

・使える機能の制限

などを行っている。

3．管理業務の一例

さる、2001年9月19日の早朝より三重大学外へのホームページの閲覧が行えない状態がしばらく続きました。通常のネットワーク接続ユーザは何時ものことかと思われたかもしれませんが、全学のネットワーク管理者は早期復旧を目指して様々な対応を行っていました。各種サーバをはじめルータ等も含むネットワーク管理がどのように行われているかを、コンピュータウイルス（Nimda）の感染・発症に対する全学及びネットワークグループの対応を紹介します。

なお、全学の対応例はネットワーク管理者のメーリングリストに流れてきたメールを基にまとめましたので、完全なものではありません。また、現在のネットワークグループのメンバーでは、全学のネットワーク管理者向けのメーリングリストに登録されているわけでは無く、一部の情報しか収集しておらず、参考程度として下さい。

3.1 コンピュータウイルス Nimda

コンピュータウイルスNimdaは2001年9月17日（トレンドマイクロ社ホームページより）に発見された、多数の感染方法を持つ大量メール送信型ワームである。発生後1週間で、国内434件、世界では143万5,675台のコンピュータの感染が報告されたように、非常に感染力が高いウイルスである。

また、三重大学内でも多数のサーバ（ほとんどがMicrosoft社のIISと思われる）やWindowsパソコンが感染・発症したようである。なお、IISとはMicrosoft社のWindows NT,2000上で稼動するインターネットサービス（メール等）を提供するサーバソフトの総称である。

次にNimdaの感染対象、感染方法及び発症後の動作を以下に示す。

○ 感染対象

Micirosoft社のWindows 98,Me,NT,2000及びIIS

○感染方法

・メールに添付して進入

添付されたNimdaを直接開かなくても、IEのセキュリティホールにより Outlook（メーラソフト）などでブラウズするだけで感染・発症。

・ホームページ上から進入

IEのセキュリティホールにより、Nimdaに感染したホームページを閲覧するだけで、Nimdaをダウンロードし実行してしまい感染・発症。

・ネットワーク共有サービスより進入
アクセスできる総てのMicosoftのネットワーク共有サービスを探し出し、自分自身をコピーする。知らないうちにそのファイルを開いてしまうと感染・発症。

・IISのセキュリティホールより進入
IIS のセキュリティホールを利用して自分自身のコピーを転送、実行することにより感染・発症。

・ウイルス(CodeRed)が仕掛けたバックドアより進入
CodeRed （Nimdaより以前に流行）が作成するバックドアを探してそこから自分自身のコピーを転送、実行することにより感染・発症。

○発症後の動作

・自分自身を添付したメールの送信
Outlook を起動し、アドレス帳に登録されている相手先に対し自分自身を添付したメールを自動送信する。

・ホームページを改変
感染・発症したサーバがWebサービスを行っていると、自分自身を実行するようなスクリプトをhtmlファイルを改変して埋め込む。

・共有ネットワークを探して自分自身を転送
感染したマシンからアクセスできるファイル共有サービスを探し出し、自分自身のコピーを転送する。

・IIS のセキュリティホール、CodeRed のバックドアをスキャンし自分自身を転送

3.2 全学での対応

情報処理センターを中心とした各ネットワーク委員の対応の様子を以下のように推察したものを以下に示します。

・2001年9月18日深夜頃から発症したNimdaが他のIISをスキャンを開始したため、多量のhttpアクセスによるネットワークのトラフィックの上昇が始まる。

・19日早朝の段階ではトラフィックの上昇に加え、学外に対しても多量のスキャンが認められたため、管理者向けのメーリングリストにて注意喚起が行われた。

・しかしながら、発症したサーバの活動がなかなかで停止しないため、感染・発症したサーバの特定作業が情報処理センター及び各ネットワーク委員で行われた（メーリングリストからの情報によると19台)。

・特定されたサーバの管理者に対し更に勧告が行われた。また、連絡がつかない又は管理者が不明のものもあったため、学部の管理者によっては緊急避難的に Giga-SW の停止を行ったところもあったようである。

・情報処理センターでは、活動が停止しないサーバのフィルタリング設定行い学外、他部局との通信を遮断。

・ネットワーク管理者に対しメーリングリストにて Windows パソコンの感染に対する注意喚起が行われた。

この様な作業が行われ 20 日中には、ほぼ Nimda の活動を停止させることが出来たようである。

3.3 ネットワークグループでの対応

ネットワークグループでもメーリングリストからの情報により、直接管理しているサーバ、パソコンの感染の有無を調査し、感染していないことを確認した。また、就職情報室のパソコンに関しては、IEのセキュリティホールの対策やウイルス対策ソフトの定義ファイルのアップデート等を行い、今後に備えた。

次に工学部 Web サーバに対する Nimda からのスキャンを報告する。

Nimda は IIS のセキュリティホールや CodeRed のバックドアを調べるために1回のスキャン付き

20 回弱のアクセスを行う（図２）。そのため、かなりのアクセス量となりトラフィックの増大に繋がったようである。また、総アクセス数に対する Nimda アクセス数の比較（図３）とアクセスしてきたサーバ（Nimda により感染・発症）のアクセス数（図４）に示す。

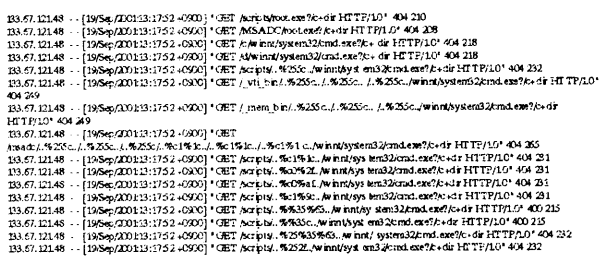

図２　Nimda からのアクセス例

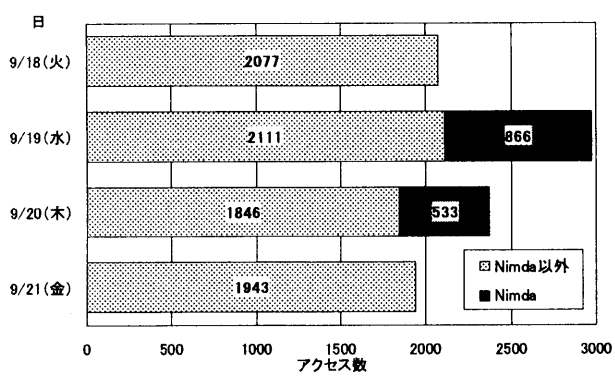

図３　アクセス数に占める Nimda の割合

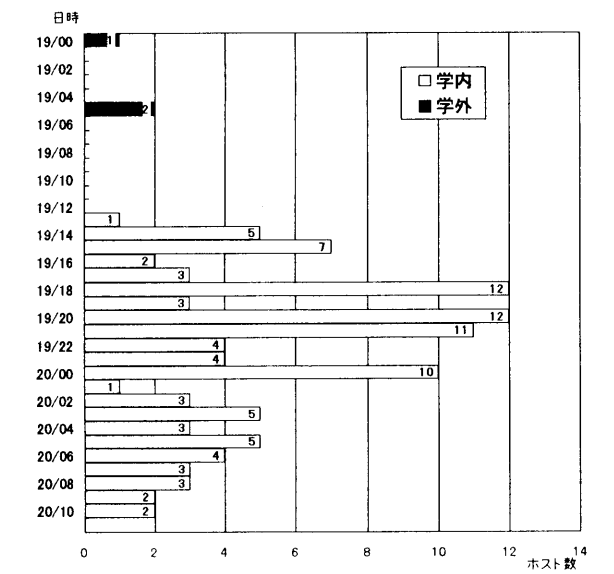

図４　アクセスしてきたサーバ数

3.4 パソコンにて感染・発症した Nimda の駆除

2001 年 9 月 20 日の朝、工学部の事務部よりネットワークグループに対し、「パソコンのアプリケーションソフト（Excel）が起動しないので一度見てほしい」との要請があり、担当者が状況を調べてみるとコンピュータウイルス Nimda に感染していることが確認された。そこで、ネットワークグループのウイルス対策チームによる駆除が行われ、無事に駆除することに成功した。以下に、Nimda の駆除作業を報告する。なお、感染したパソコンの OS は Windows 98 である。

・20 日朝、工学部事務部よりネットワークグループに対し「アップリケーションソフト(Excel)が起動しないので様子を見てほしい」との要請があり、連絡を受けたメンバーが状況を調査。

・その結果、動作がコンピュータウイルス Sircam の感染例と似ていたことから、ネットワークから当該パソコンを切り離し、Windows のレジストリのチェックを行うとともに、ウイルス対策ソフトメーカのホームページから情報を収集して調査した結果、コンピュータウイルス Nimda と判明した。この時点でネットワークグループで使用しているイントラネットソフトウェア(Sky Board)にてメンバー全員に対して報告を行い、その結果ウイルス対策チームで対応にあたることになった。

・そこでウイルスの駆除方法を検討し、最善の方法は OS、アプリケーションソフトの再インストールであるが、パソコン内に把握しきれない（代々引継ぎがうまく行われてこなかった）重要と思われるデータファイル等が存在するので、ワクチンソフトで行うこととした。

・パソコンにはウイルス対策ソフトのプリインストール版が存在したが、ライセンス期間が過ぎていたため最新の定義ファイルを使用することが出来なかった。そこで、シマンテック社のウイルス対策ソフト(Norton AntiVirus)の試用版を用いて最新の定義ファイルを用いることと

した。

・他のパソコンから使用版のダウンロードを行ったが、ファイルサイズ大きく対象パソコンの外部記憶装置では扱えないことから、一時的にファイル共有を行いソフトウェアを転送することとした。その際、当該パソコンにてファイル共有フォルダを作成した際に、早速 Nimda 自身のコピーされたファイルが現れるという情報通りの結果を確認できた。また、事前に手動にて Nimda の活動を停止しておいたが、停止していないことが判明した。

・次に試用版のウイルス対策ソフトのインストールを行ったが、ドライブ C:の空き容量が無いためドライブ D:にインストールを行った。つぎに最新定義ファイルを用いて Nimda の駆除を開始し、2 時間後に 1,976 個の感染ファイルの検出及び駆除を行った。次に 2 回目のチェックを行ったところ、更に 30 個の感染ファイルを検出し駆除を行ったが、完全に活動を停止できていない事が判明した。

・そこでトレンドマイクロ社がホームページ上で無償で提供している Nimda 専用の駆除ツールを用いて作業を行い、新たに 5 個の感染ファイルの検出及び駆除を行い 19 時過ぎに総ての作業を完了した。

・翌 20 日に再び工学部事務部より「Outlook でメールを送信しようとしたら警告メッセージが現れた」との連絡があった。そこで、至急ネットワークケーブルを外してネットワークからの切り離しを行う旨の指示を行い、調査した結果昨日インストールしたウイルス対策ソフトが Nimda の活動を検出したためと判明した。

・今度はシマンテック社がホームページ上で無償で提供している Nimda 専用の駆除ツールを用いて作業を行い、午前中にようやく Nimda の駆除に成功した。

後ほど、ホームページ上で情報を収集したところ、Nimda の感染が進んだ場合は完全な駆除が出来ないなどの事例が報告されていた。OS、アプリケーションソフトの再インストールはある程度の時間はかかるが、その時間内には完了する。また、感染したウイルスを完全に駆除できるので特別な理由がない限り、再インストール行うことを進める。

できれば、ウイルスからの感染を事前に防ぐためにもウイルス対策ソフトの導入・運用、または怪しいメールの添付ファイルを開かないなどの日ごろからの注意も必要である。

4．さいごに

グループウェアをはじめとするイントラネットによる業務が拡大していく中、ネットワーク関連の管理の重要性は増すばかりである。その中でも被害が大きい、ネットワークセキュリティへの対応はネットワーク管理者のみならず、パソコンユーザも高い意識を持たなければならない。

Nimda の例が示すように、情報処理センターも様々なセキュリティ対策を行っているが、もともとファイアウォールは外部に対しては有効に働いても、ネットワークの内側に侵入を許すと効果は無くなる。

ネットワークグループとしてもネットワークセキュリティへの新たな対応を行うとともに、パソコンユーザへの注意喚起を兼ねたセキュリティ関係の講習会を開催するなどして全体としてのセキュリティを高めていく活動を行って行く必要がある。

参考文献

1) 山本好弘、平山かほる、“ネットワークグループの現状報告及びホームページのアクセス解析”、三重大学工学部技術部、技術官等による技術報告集　第 9 号、pp.22-28 (2001.3).

2) “ゼロから学ぶクラッキング対策”、アスキー、Linux magazine　2002 年 1 月号、pp.45-69 (2001.12).