工学部技術部　技術講習会

データファイルを守るには

日常のコンピュータの管理について

平成13年12月14日　第1系第1班　新美治利

はじめに

- もし、あなたの送ったメールにコンピュータウィルスが潜んでいたら？
  - 他の大学・企業の人たちはウィルスに感染したメールを送りつけるようなところは信用しません。
  - ウィルスによって業務支障が発生した場合は、メールの発信者に対して責任を追及されます。

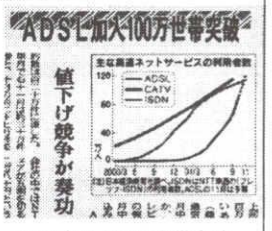
講習内容

- 三重大学内ネットワークについて
  ・インターネットについて
- コンピュータの取り巻く環境
- データを守るには
  ・ウィルス対策
  ・データのバックアップ
  ・コンピュータの管理

三重大学のネットワーク

インターネットの歴史

- 1969～1970
  軍事利用としてARPAnet
- 1980
  研究開発利用
- 1990
  インターネット登場
- ～現在
  ASDL・CTVによる
  常時接続・高速通信



ADSL加入100万世帯突破
12月11日付　日本経済新聞

三重大学のネットワーク

Giga Bit network

- Giga Bit networkの整備によって、研究用LAN・事務用LAN・学生用LANの３系統ネットワークが構築されました。
  同じネットワーク網を使いながら、全く別のLANを構築しています。
- 二重化による障害発生時のバイパス整備。

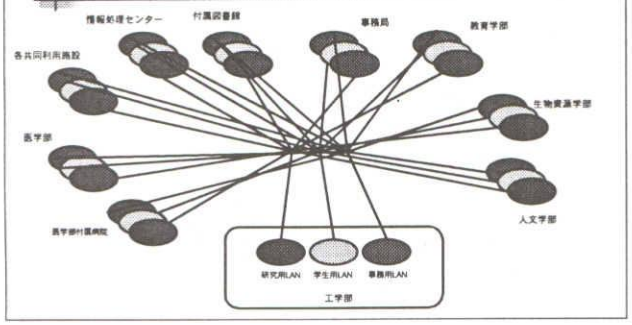
三重大学のネットワーク

研究用・学生用・事務用LAN

- 研究用LANは、IPアドレスはグローバルIPを割り振られ、世界中のどこかでも特定できるIPアドレスを使用しています。
- 事務用LANは全学事務の機器をつなぐことによってデータ共有、外部からハッキング行為を防ぐ役割もある。
- 学生LANは、学生個人のPCをネットワークに接続できる。（情報処理センターで利用講習会が行われている。）

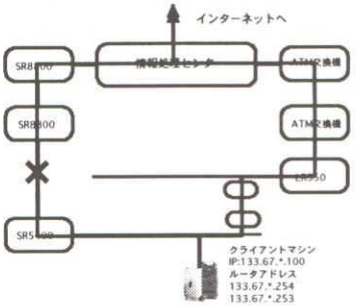
三重大学のネットワーク

研究用LAN



三重大学のネットワーク

ネットワーク二重化



コンピュータの取り巻く環境

- Windows95の発売
- コンピュータの低価格化
- インターネットの普及
  （CTV,ASDLによる高速化、
  接続料の低価格化）
- ユーザの増加
- 常時接続によるクラッカーからの被害
- コンピュータウィルスの被害の増大

コンピュータの取り巻く環境

ネットワークにつなぐと

- 電子メール
- ホームページの閲覧
- ネットショッピング
- データのダウンロード

と便利に使っていますが

コンピュータの取り巻く環境

ネットワークにつなぐと

- サーバはアクセスした内容を記録しています。

インターネット

ハッキング

- ポートスキャン
- バックドア
- 個人情報の奪取
- これらは、サーバならず、常時接続の個人のコンピュータもターゲットになります。

インターネット
クラッカー

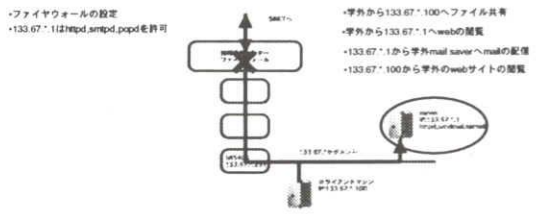
- クラッカーはハッキングを行なった上で相手に被害を加える人たちです。
- コンピュータへ侵入
- データの改ざん
- データの盗聴
- 他人になりすます
- コンピュータを破壊
- 他人の活動を妨害
- コンピュータウィルス

インターネット
ハッキングを防ぐには

- ネットワークにつながない
- つなぎっぱなしにしない
- 不要なポートの遮蔽
- ファイヤウォールを導入

ファイヤウォール

¥ 三重大学に導入されている事例



インターネット
コンピュータウィルス

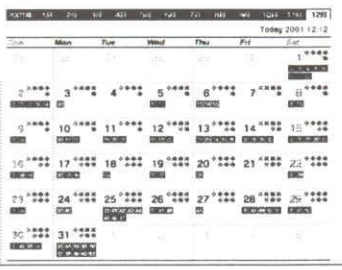
- コンピュータウィルスの種類
  - ・マクロ型
  - ・ファイル感染型
  - ・ワーム型
  - ・Java・ActiveX型
  - ・メモリ常駐型

インターネットの歴史
コンピュータウィルス

- コンピュータウィルスの種類
  - ・マクロ型
  - ・ファイル感染型
  - ・ワーム型
  - ・Java・ActiveX型
  - ・メモリ常駐型

インターネット
ウィルス・カレンダー

Virus Calendar ウィルス・カレンダー



- シマンテック社 ホームページより

インターネット
ウィルスの危険度・被害

top threats

月間ウィルス被害ランキング（2001年11月・国内）

順位	ウィルス名	今月検出	前月順位	前月検出	種類
1	W32.Badtrans.B@mm（バッドトランス）	1,004	-	1	ワーム
2	W32.Aliz.Worm（アリズ）	865	-	1	ワーム
3	W95.Hybris.worm（ハイブリス）	183	1位	1	ワーム
4	JS.Exception.Exploit（エクセプション・エクスプロイト）	110	2位	1	トロイの本集
5	W32.Sircam.Worm@mm（サーカム）	59	3位	1	ワーム
6	W32.Nimda.E@mm（ニムダ）	57	7位	1	ワーム
7	W32.Nimda.exe(dr)（ニムダ）	50	-	1	ワーム
8	W32.Badtrans@mm.enc（バッドトランス）	41	-	1	ワーム
9	W32.Nimda.enc（ニムダ）	29	4位	1	ワーム
10	W32.Klez.gen@mm（クレズ）	28	-	1	ワーム

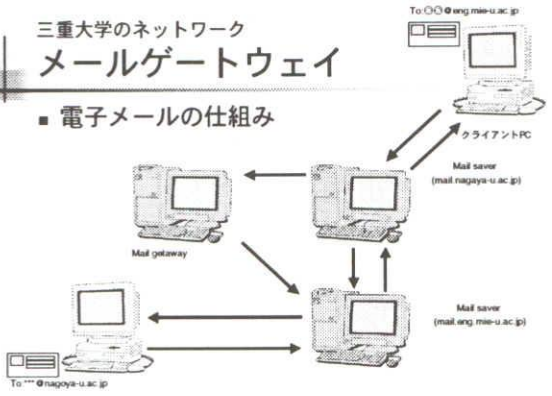
- シマンテック社ホームページより

インターネット
ウィルスに感染すると

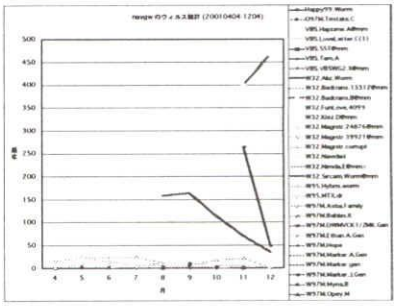
- コンピュータが起動しない
- コンピュータが正常に動作しない
- コンピュータの動作が遅くなる
- ウィルス付きメールを勝手に送信する

三重大学のネットワーク
メールゲートウェイ

- 電子メールの仕組み



三重大学のネットワーク
メールゲートウェイ

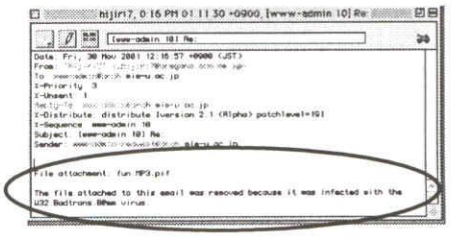


三重大学のネットワーク
メールゲートウェイ

- 定義ファイルにある既知のウィルス
  修復可能なものは修復して配信する。
  修復不可能のものは削除する。
- 定義ファイルにない未知のウィルス
  検出不可能のものは素通りする。

三重大学のネットワーク
メールゲートウェイ

- 既知のウィルスを削除した例

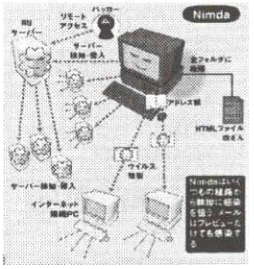


データを守るには

- コンピュータウィルスの対策
- Nimdaの駆除について
- データのバックアップ
- 日頃のコンピュータ管理

NIMDAの感染方法

- ホームページ閲覧
- メールの送受信
- ネットワーク経由
  ファイル共有



NIMDAの症状

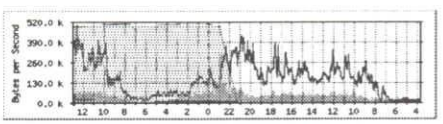
- クライアントコンピュータ
  ・感染したファイルを添付してメールの配信
  ・ハードディスク内に感染したファイルを増殖
  ・ファイル共有を自動に設定する。
  ・システムの初期設定を書き替える。
- サーバ
  ・他のサーバへ攻撃
  ・ハッカーに乗っ取られて、データの改竄

NIMDAの予防策

- 1台のコンピュータを駆除に要した日数は2日間掛かりました。日頃コンピュータをメンテナンスしておけば、短い時間ですんだと思われます。

学内でのNimdaの被害

- ネットワークの障害
  2001.9.18 PM10:00ー



三重大学ノード-学術情報センター間トラフィック
（三重大への入力が青、三重大からの出力が緑で表示）

学内でのNimdaの被害

- Webサーバへアクセス集中

Nimdaの駆除作業

- 2001年9月20日に行われたNimda駆除作業について報告します。
- 作業依頼
  日時：2001.9.20　AM9:00
  依頼者：事務系職員
  該当機種：DOS/V機　Windows98
  内容：コンピュータのアプリケーション
  の異常な動作が起こる。

Nimdaの駆除作業

- AM 9:00　電話の内容から、ウィルスに発症した兆候だったので、LANのケーブルを抜くことを指示しました。（２次感染防止）
- AM 9:15　現場に出向き、状況を確認しました。デスクトップ上のショートカットでアプリケーションを起動すると、README.EXEファイルが開かれる。

Nimdaの駆除作業

- この時点では、経験により、Navidadと判断、レジストリの内容をチェックしたが、該当項目の変更はされていなかった。
- AM 10:00　テレビのニュースでNimdaを取り扱っていたので、Nimda・Sircamに関する情報収集を行った。

Nimdaの駆除作業

- redame.exe ・filename.eml等のW32.Nimdaの特有のファイルを発見
- AM 10:15　W32.Nimdaはsystem.iniを次のように改変します。
  Shell= explorer.exe load.exe -dontrunold ->Shell= explorer.exeを 書替
  Riched20.dllファイルを置き換えを行った。

Nimdaの駆除作業

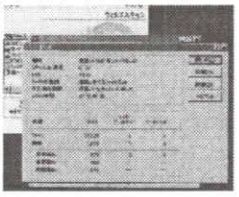
- AM 10:45　Norton AntiVirusの試用版を入手したが当該PCには、MOなどの装置がないため、一時的にネットワークに接続し、ソフトのコピーを行なった。
- その際も、当該PCはウィルスによってに共有設定が行われておりの新規作成の共有フォルダー内にはredame.exeが作成されていました。

Nimdaの駆除作業

- PM 11:00　当該PCにインストールを行ったが、Cドライブの空き容量がなく、インストールができなく、容量確保の作業を行った。
- PM 0:00　結局Dドライブインストールし、スキャンを開始

Nimdaの駆除作業

- PM 2:00 1回目スキャン終了1976個の感染したファイルを検索し削除行った。
- PM 3:15　2回目のスキャン終了30個の感染したファイルを検索し・削除行った。



Nimdaの駆除作業

- PM4:00 ウィルスの活動停止できなかったので繁殖をはじめ、トレンドマイクロ社W32.Nimdaの駆除ツールを使い、駆除を行った。
- PM6:00 3回目のスキャン終了5個の感染したファイルを検索し・削除行った。
- PM7:00 作業終了

Nimdaの再発

- 2001.9.21AM8:45 再び、Out Look expressを起動するとAnti Virusから警告がでると連絡を受け、現場へ
- AM 9:00 Anti Virusから警告は、「README.EXEを添付して送信していいですか」でした。
- AM10:00 W32.Nimda.A@mm駆除ツール入手して、駆除を行った。

Nimdaの再発

- AM10:00 シマンテック社のW32.Nimda.A@mm駆除ツール入手して、駆除を行った。
  結果、1500の感染ファイルを検索・削除した。
  2回検索を行い、削除を行った。

二日もかかった駆除作業

- 前任者から引き継がれたままで、HDのメンテナンスがされてなかった。
- バックアップの有無が確認できなかったので、データを保持しながらの作業であった。

コンピュータウィルスの対策

- ウィルスに感染しないために
- ウィルス情報の入手方法
- ウィルスチェックソフトの導入
- ウィルスチェックソフトから警告
- いつもと違う感じがしたら

ウィルスに感染しないために

- 知らない人からのメールは開かない。
  最近は、アドレス帳を利用して送信するものが多い。
- 見覚えのないファイルは開かない。
- ウィルスチェックソフトを導入する。

ウィルス情報を入手

- セキュリティ・ウィルスに関する情報サイト
  コンピュータ緊急対応センター
  http://www.jpcert.or.jp/
- ソフトメーカーのウィルスに関する情報サイト
  シマンテック(Norton Anti Virus)
  http://www.symantec.co.jp/
  トレンドマイクロ(ウィルスバスター)
  http://www.trendmicro.co.jp/

ウィルスチェックソフトの導入

- ウィルスの感染を防ぐには
  ネットワークにつながない・データも交換しないことが、一番の得策ですが、研究活動をしていく上ではデータ共有は不可欠です。
- ウィルスチェックソフトの導入
  Norton AntiVirus・ウィルスバスターなど

ウィルスチェックの対象

- メールの添付ファイル
- フロッピーディスクなどのメディア
- Webブラウジングなどの一時ファイル
- FTPなどのファイル転送

などの外部から保存されるファイルに対してチェックをします。

ウィルス警告がでたら、

- 感染ファイルをコンピュータに取込んだ場合
  ウィルスの感染したファイルの削除・隔離
- ウィルスが感染した場合
  ネットワークケーブルを抜く。
  ウィルススキャンを行ないウィルスの感染したファイルの削除・隔離をおこなう。
  徹底的にウィルスを駆除する。

いつもと違う感じがしたら

- スタートアップの設定がしてないのにソフトが立ち上がる。
- 覚えのないファイルができている。
- ソフトウェアが起動しなかったり・起動して不自然な動作を行う。

日頃とは、違う様な感じがしたら、ウィルスチェックすることを勧めます。

データを守るには

- コンピュータウィルスの対策
- データのバックアップ
- 日頃のコンピュータ管理

データの破損・消失

- 日常、コンピュータを使用していてもファイルの破損・消失がありえます。
  - ・上書き保存
  - ・停電
  - ・フリーズからのリセット
  - ・接続ケーブルの不良
  - ・プログラムの強制終了
- FD・HDの損傷です。

データファイルの扱い

- 大事なファイルを守る方法には
  ハードディスクへの一時保存
  メディアへの保存
  ファイルサーバへの保存

ファイルの一時保存

- ファイルサーバなど必要なファイルや作業中などのデータは一時的にからハードディスクへ保存する。
- ファイルサーバと接続したままにしない。
- フロッピーなどの書込回数が増えるとディスクの破損につながる。
- 作業進行中のファイルは作業ファイルを作成して、元のファイルを保護する。

メディアへの保存

- フロッピーディスクなどへデータの保存
  作業終了や終業時に、保存用として書込回数を少なくする。
  メディアの保管には、磁気・温室度以外にも盗難にも注意をする。

ファイルサーバへのデータ保存

- 作業終了や終業時にデータを転送する。
  ファイルサーバは、ネットワークで各コンピュータ接続されているので、管理を怠らない。クライアントはアカウント・パスワードで接続し作業終了したら接続を切る。

ファイルサーバへの データ保存の危険性

- コンピュータウィルスの感染したファイル入り込むと、蔓延しかねない

データの復旧

- 破損・消失したファイルは復旧はほとんど不可能です。
- ユーティリティソフトで復元できることがあります。必ずしも万能ではありません。
- データのバックアップをとることが大切です。

データを守るには

- コンピュータウィルスの対策
- データのバックアップ
- 日頃のコンピュータ管理

コンピューターの管理

- 日頃からコンピュータをみることによって
  ・ウィルスの被害
  ・データの損失
  ・ハードウェアの故障
  など、未然に防ぐことができ、
  ソフトウェアの修正ソフトを当てることによって使いやすい状態になります。

コンピュータに関する情報

- ハードウェア・ソフトウェア
  メーカのホームページに
  ・修正・バージョンアップ
  ・テクニカルな情報
  ・トラブルシューティング
  などの情報が掲載されています。

コンピュータを起動時

- コンピュータの電源が入れる前に周辺機器の電源を入れる。
- コンピュータの電源が入れる。
- コンピュータから異音・異臭がしたら、直ちに使用をやめる。

アプリケーションが固まったら

- Appleの場合
  - ・Command+S(File save)
  - ・Command+Q (Quit)
  - ・Command+option+esc(ソフト強制終了)
  - ・Command+Control+電源（ソフトリセット）
- Windowsの場合
  - ・ Alt+Control +delete(タスクマネジャーを起動)
  - ・アプリケーションを強制終了

コンピュータを終了時

- アプリケーションを終了させる。
- メニューにある終了で、コンピュータを終了させる
- コンピュータの電源がきれた後に周辺機器の電源を切る。

提案

- メールでの添付ファイルを行う場合は、本文中にファイル名・データのサイズを書き込む。
- 定期的に定義ファイルの更新を行って下さい。

まとめ

- 今回、学内のウィルス感染したコンピュータの大半は、使用者のウィルス等危機感の低さが、被害が増大したと思えます。
- 自分のデータは自分で守ることは、周りに迷惑をかけないことにつながります。

最後に

- 今回、講習会の資料作成には、情報処理センターの杉浦先生・工学ネットワーク管理委員会の先生方のご協力を賜りありがとうございました。