ネットワークセキュリティ

2004/06/28

芸術情報設計学科
藤村　直美

概要

- ネットワークセキュリティの概要
- 情報基盤室（昔の情報処理センター）が行ってきた対策
- 利用者が気をつけるべき対応

攻撃パターン

- メールに添付されたウイルス
  - ファイルの自動実行機能を悪用
  - 最近はプレビューしただけで感染
- ファイルのダウンロードによるもの
  - ブラウザ側で自動的に実行した結果
    - 効果が即時に影響が出現するもの
    - 潜伏して後で影響が出現するもの
- ネットワーク経由で直接攻撃
  - サーバのセキュリティホールを利用

コンピュータウイルス

- 1988年に出現？
- 感染経路
  - メール
  - ファイルのダウンロード
  - 直接攻撃
  - これらの複合パターン
- 日本ではIPA　に届けることになっている
- 届け出件数は激増しているが、本当に届けているか？

ウイルスの分類

- ファイル感染型
- マクロ感染型
- トロイの木馬型
- システム領域感染型
- 複合感染型

ファイル感染型

- 拡張子com、exe、sysなどの実行型ファイルに感染するもの
- 実行可能プログラムに付着して制御を奪い、感染・増殖
- 先頭や末尾に付着、隙間に挿入、上書きなど
- Internet ExplorerやOutlook Expressなどの自動実行機能を悪用

マクロ感染型

- Excel、Wordなど、マイクロソフトのアプリケーションのマクロ機能を利用
- 機種やOSに依存しないで感染
- マクロを実行しないというセキュリティ機能を使って防げる
- W97_MELLISA（メリッサ）はOutlookのアドレス帳に登録されている宛先にウイルスを送信

トロイの木馬型

- 増殖を目的としない不正プログラム
- 自己完結型
  - ファイルの破壊など致命的な活動
  - 一回限り
- サーバ＝クライアント型
  - パスワードを盗む
  - マシンを遠隔操作する
    (DDoS：Distributed Denial of Serviceなど)

システム領域感染型

- HDやFDのシステム領域（ブートセクタ、パーティションテーブル）に感染
- 何よりも最初に実行される
- メモリに常駐する
- 最近は少なくなった

最近のウイルス

- MTX
- MAGISTR
- HAPTIME
- GONE
- BadTrans
- Zoher
- SIRCAM
- NIMDA
- CODERED
- Aliz
- AGENT
- PLEXUS
- BBA
- ZAFI
- SDBO
- KORGO

ウイルス詳細

- SIRCAM
  - 自身のコピーをメールに添付
  - 「マイドキュメント」フォルダーから無作為にファイルを添付
- NIMDA
  - メールの添付ファイル、プレビューだけで感染
  - Webブラウザで表示するだけで感染
  - IISサーバのセキュリティホールを利用
  - 共有ドライブへのコピー

ウイルス詳細

- CODERED
  - HTTPリクエストでコピーを転送
  - バッファオーバーフロー攻撃を行う
  - メモリ上で直接実行、ファイルに痕跡が残らない
  - 1～19日はランダムないPアドレスを攻撃
  - 20～28日はホワイトハウスをDoS攻撃
  - 29～31日は何もしない

ウイルス詳細

- Aliz
  - Internet Explorerのセキュリティホールを利用
  - Outlookではプレビューだけで感染
  - Outlook Expressのアドレス帳に記載されている全アドレスにウイルスを添付したメール送信

ウイルスデマ情報

- 必要なシステムファイル（例えばSULFNBK）をウイルス呼ばわり
- 存在しないウイルスに対する脅威
  - 大企業の名前をかたり、信頼性をあげる
  - チェーンメール的に転送させる
  - 大げさなことが書かれている
- デマ情報は読んだだけでは感染しない

ウイルス対策5箇条

- ウイルス検出ソフトウェアの導入
- パソコンをデフォールトの設定で使わない
- セキュリティパッチを適用
- 感染の兆候を見逃さない
- データをバックアップ

ウイルス検出ソフトウェアの導入

- メーカは問わない
- TrendMicroのウイルスバスター2004は
  - リアルタイム監視
  - メールの添付ファイル監視
  - ダウンロードファイル監視
  - 危険なＵＲＬの監視
  - パーソナルファイアウオール
  - 定期的なボリューム検索

ウイルス検出ソフトで重要なこと

- ウイルス検出機能を有効にする
  インストールするだけでは駄目
- パターンファイルを常に最新に更新する
  頻繁に更新される

セキュリティ強化法

- メールの添付ファイルは開く前にウイルス検索を行う
- ダウンロードファイルはウイルス検査を行ってから開く
- フロッピーでやり取りする時も注意
- パソコンを貸した時も注意
  (ネットワークに接続する前にチェック)

デフォールトで使用しない

- Internet Explorerのセキュリティレベルを「中」以上に設定する
- Word、Excelなどのマクロ機能をoffにする
- マクロウイルス警告を有効にする
- 全ての拡張子を表示させる
- Windows Scripting Host(WSH)あるいはVBSの機能を無効にする

セキュリティパッチ

- OSごとにセキュリティホールを塞ぐためのソフトウェアが提供される
- Windows Security Updateをこまめに点検しておくと自動的に更新可能
- 関連情報をこまめに点検する
  - IPA、JPCERT
  - 警察庁
  - Microsoft など

感染の兆候を見逃さない

- 動作速度が遅くなる
- メモリが不足する
- 画面に覚えのないメッセージが表示される
- 画面上の文字が崩れる
- データが壊れる
- アイコンが変更されている
- プログラムが起動しなくなる
- 知らないファイルができている
- プログラムファイルの大きさが大きくなる
- 覚えのないメールが送信されている
- 勝手にインターネットに接続する
- ダイアルアップの接続先が変更される (海外など)

データのバックアップ

- 日頃からこまめにバックアップする
- バックアップする前にウイルスに汚染されていないことを確認する
- バックアップした媒体はオフラインになっていることが望ましい
- 簡単に取り外せる記憶媒体の活用

センターにおける二つのウイルス対策

- 情報システム管理運用委員会で議論
  (平成13年12月)
  - 電子メールにおける添付ファイルに対するウイルスチェック機能の導入 (平成13年11月)
  - トラヒックフィルタリングの強化 (平成14年1月)

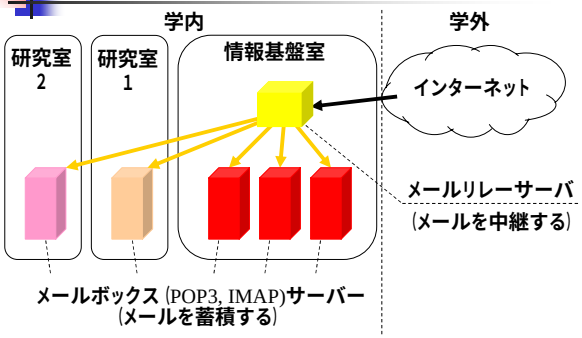
ウイルスチェック機能と効能

- 目的
  学外から学内へ届くメールによるウイルス感染を防ぐ。本学から学外へ送出されるメールによるウイルス感染を防ぐ。
- 動作
  電子メールに添付されるプログラムがウイルスであるかどうかをチェックし、ウイルスであった場合それを取り除く。
- 効能
  ことにより本学におけるウイルスの蔓延を防ぐ。

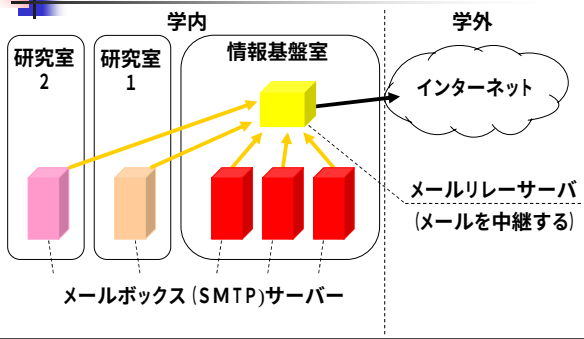
メール配送のしくみ

- インターネットにおけるメール配送
  - バケツリレーで届く
  - あて先アドレスで次の行き先が決まる
- 学外から学内あてのメール配送
  - あて先アドレスが、次の形式であるもの
    ○○○@design.kyushu-u.ac.jp
    △△△@□□□.design.kyushu-u.ac.jp
  - 学外からは、かならず情報処理センターのサーバ（メールリレー）に届く。
  - メールリレーは、学内の適切なメール（ボックス）サーバに届ける。

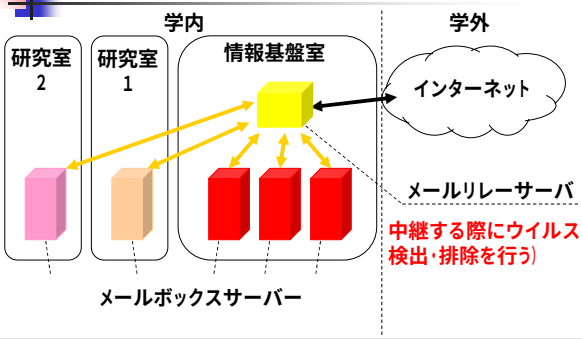
メール配送のしくみ（学外→学内）



メール配送のしくみ（学内→学外）



ウイルスチェック機能



注意事項

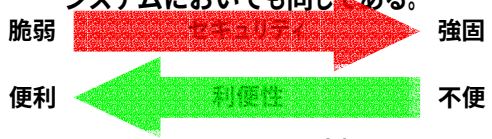
- ウイルス検出は完璧でない（ウイルスを認識できない場合がある）
  - パターンファイルの不備
    - 解析と対応がまだ終わっていない
    - 更新が間に合っていない
  - こわれかかったメール
    - パターンファイルには引っかからないがウイルスとしては機能

利用者から見ると

- ウイルスメールが来たという通知（メール）が、ウイルスチェックサーバから届く。
- メールの本体は来ない。

コンピュータネットワークとセキュリティ

- セキュリティ：守るべきものを守ること。
- セキュリティと利便性は相反する。情報システムにおいても同じである。

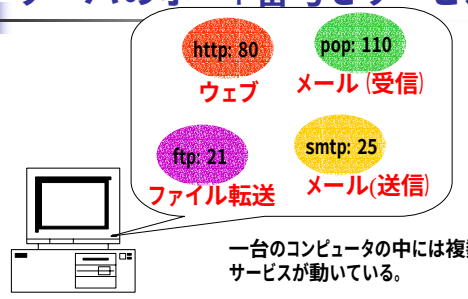


コンピュータネットワークにおける究極のセキュリティはネットワークに接続しないこと

トラヒックフィルタリング

- インターネットでは、情報をパケットと呼ばれる単位に分割して伝送する。
- パケットには、通信を行っているコンピュータの組を示すIPアドレスおよびポート番号が記されている。
- IPアドレスやポート番号を元にパケットの通過を制限することをトラヒックフィルタリングと呼んでいる。

サーバのポート番号とサービス



一台のコンピュータの中には複数のサービスが動いている。

トラヒックフィルタリング（従来）

- ねらわれやすいポートへの通信を遮断
  - 第1フェーズ（1996年1月）
    telnet, tftp, smtp
  - 第2フェーズ（1996年8月）
    +pop2, pop3, login, nfsd
  - 第3フェーズ（2001年2月）
    +echo, chargen, ssh, whois, domain, finger, sunrpc, netbios-*, exec, shell, printer, uucp, callbook, canna, x11,
  - …

だんだん強化してきたが、これでは現実的ではない状況になった。

現実的ではない理由

- これまでのやり方は現実的ではない
  - 攻撃の増大
    - 人間の手作業による攻撃から、マシンを利用した攻撃（自動化）
  - 相手を特定しない無差別な攻撃の増加
  - 非力なマシンは、攻撃により速度低下などを起こす。

ポリシーの改訂

- これまでのトラヒック制限
  ねらわれやすいポートへの通信を遮断
- これからのトラヒック制限
  原則として、業務上必要な通信のみ通過させる。(すなわち、その他のトラヒックは通さない)

利用者に望まれること

- ウェブサーバはできるだけ情報処理センターのものを使用する。
- 研究室でのウェブサーバを運用する場合は、できるだけひかえる。
- 万一、研究室でウェブサーバを運用する際は、情報処理センタにファイアウォールの設定変更を依頼し、セキュリティ対策を随時行い万全の体制で運用を行う。
- 不必要なサーバは(その機能を)停止する。

利用者における対策

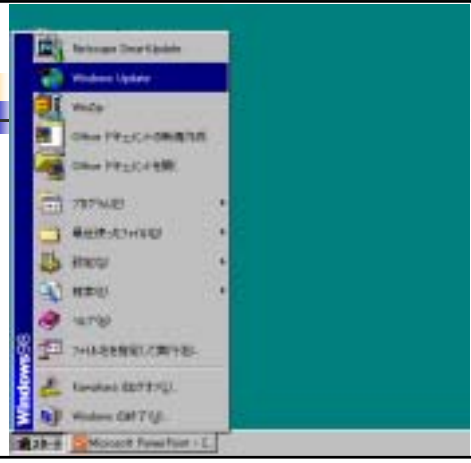
- 世の中の動向(日々参照すべきWeb)
  - 文部科学省大臣官房政策課情報化推進室
    http://shinko-www.mext.go.jp/security/
  - 情報処理振興事業協会(IPA) セキュリティセンター
    http://www.ipa.go.jp/security/
  - JPCERT(コンピュータ緊急対応センター)
    http://www.jpcert.or.jp/ (メーリングリストがあります)
  - 警察庁ハイテク犯罪対策
    http://www.npa.go.jp/hightech/

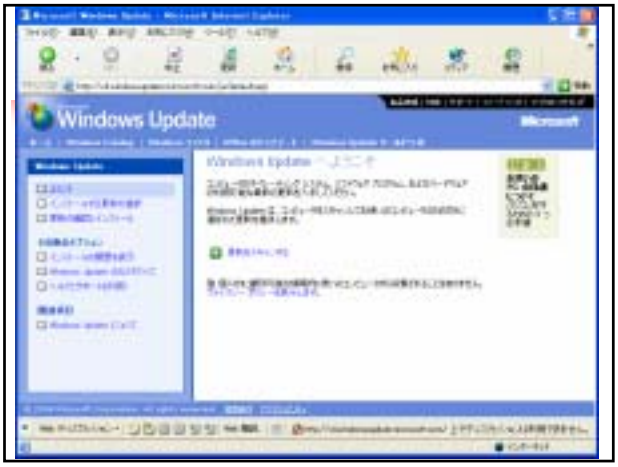
情報収集(お勧め)

- jimuウェブ
  http://www.design.kyushu-u.ac.jp/~jimu/
  - 芸工大の事務のページに関連リンクが整理されています
  ご利用ください。(学内ポータルページ)
- 中村正三郎さんのページ
  (河原の個人的おすすめ)
  http://www.asahi-net.or.jp/~KI4S-NKMR/

日常の健康管理(これが一番)

- OSやソフトウエアの更新(パッチを当てる)
  - Windows Update(Windows98以降)
  - マイクロソフトオフィスの修正ファイル
  - Linuxの RPMファイル
- ウイルスチェックソフト
  - ダウンロードするファイルやフロッピ/CDなどのファイルは、個々に対策すること
    ウイルスバスター(トレンドマイクロ社)
    アンチウイルス(ノートン社)
  - 機能をONにすること。 パターンファイルの更新





日常の対策(気を配ること)

- 不要なサービスは停止する
  - WindowsNT, 2000は要注意
    - 勝手にパーソナルウェブサーバーが稼動していたりする(セキュリティホールとなります)
    - 確認法:当該マシンにブラウザーでアクセスする
  - Unix系OS
    - inetd.conf (xinetd.conf)の整理
    - daemon プロセスの管理(samba など)

ファイル共有

- ファイル共有は便利な機能ですが、大事なファイルをみんなに見せていませんか?
- パスワードの設定/読み書き権の設定
- 自分のパソコンの共有資源の確認法
  - 自分で自分の共有資源を「検索」する

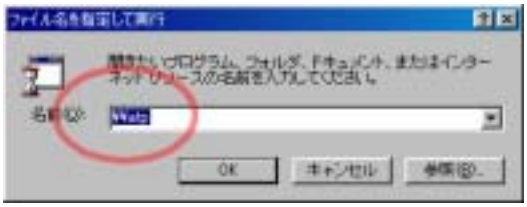
ファイル共有のパスワード

まずコンピュータ名を確認

検索のウラ技

ウラ技(続き)

- ￥￥に続いて　自分のコンピュータ名を入力して「OK」をクリック



見られてる？

やっぱり大事なパスワード

- 自分が忘れにくく、他人に推測されにくい
- 大文字･小文字･数字･記号を混ぜる
- 辞書にある単語や有名人の名前を、そのまま使わない
- 定期的に変更する。
- yppasswd 、nispasswdコマンド

学外から本学へのアクセス時に

- プロバイダ経由や他の組織から、本学へのアクセス時に注意すること

(主にメールを読むときに…)パスワードを盗み見されないように。

メイラーのおすすめ設定

- APOP　(←おすすめ)
  - POP(メールをパソコンに取りこむやり方)のユーザー認証の部分を暗号化したもの
  - /usr/local/bin/popauth コマンドで設定する
  - Outlook, Netscape は APOPに対応していない
  - AL-Mail, Eudora, Winbiff, EdMaxは対応している
  - (Outlookは、危ない?)

各メイラーのweb

- AL-Mail (http://www.almail.com/)
  教育機関は無料で使用できる
- Eudora (http://www.eudora.ne.jp/)
  Mac版で有名な Eudora. Windows版も
- EdMax (http://www.edcom.jp/)
  最近、人気があるらしい。無料版も
- Winbiff (http://www.orangesoft.co.jp/)

Outlookは危ない?

- IE と OE はWindowsに標準搭載されているために、利用者が多く狙われやすい
- 動作が自動化されているために、ウイルスを自動実行してしまう。
- OEはHTML形式のメール送信が初期設定
- Windows(98-ME)とIEの統合化を無効にするソフトウエア
  - IE-OFF
  - http://www.annoyances.org/exec/show/software からダウンロード

SSLって

これですよ

telnet する人はどうする

- SSH (Secure SH)で暗号化通信する
  - Windows の場合 Teraterm Pro
    (http://hp.vector.co.jp/authors/VA002416/)
    + TTSSH
    (http://www.zip.com.au/~roca/ttssh.html)
  - Mac の場合 MacSSH シェアウエア
    (http://www.macssh.com/)

Unix系マシン管理者にお願い

- ユーザー IDの管理
  - 学内でユニークに決まるUIDに
  - 教職員は情報処理センターで割り当て
  - 学生は学籍番号から生成
    詳細は情報処理センターで確認してください
- IPアドレスの設定の間違いがないように

さいごに

- どこか1個所でもよいですから、気に入った情報サイトをみつけて(もしくは~jimu)、定期的に(毎日、毎週)巡回してみたらいかがでしょうか
- Windows Updateを定期的におこなう