#13 アタック・犯罪・セキュリティ

Yutka Yasuda, 2003 spring term

はじめにすこし

- Networld + Interop に行ってきました
  - 毎年一回行われているネットワーク関連技術の展示会
  - 比較的先端分野のことが出てくるのが特徴
  - 今年は少し景気良い雰囲気でした
- IP Phone
  - IP Phone 対応を謳った製品やサービスが大量に出ていました
  - 来年ごろからかなり高い率で友達とNTT を通さずに電話ができるようになりはじめるでしょう
  - 相互接続性が完全でないということに注意
  - それがなくなっていく過程に、より注意を

7

updates

- 地球シミュレータの気象分析への応用
  - スーパーコンピュータの主要な応用用途
  - アメダスの設置間隔を詰めることが可能か？
- 単に高速なコンピュータがあるだけでなく
  - その応用を全体として支えている背景にも注目
- モデルに注目
  - ミクロなセンサーから情報を集めてマクロな情報を作るというモデル
  - 極めてインターネット的（名古屋のタクシー事例、マイクロノードの試聴機など）

8

9

10

12

アタック

- ネットワーク越しにシステムに侵入
  - 運用者の意図に反した振舞いをさせる
  - Web ページの改竄、データの消去、持ち出し（情報漏洩）
  - ソフトウェア構造上の不備が入口
  - セキュリティホールの修正で対応
- script kiddy による安直な攻撃
  - そこを踏み台にして更に他者を攻撃
  - Worm などの自動侵入も増えている
- 昔は「管理者たるもの」で良かった
  - 誰もがつながる世界では違う
  - 誰でも安全に運用できるものでなければならない
  - Windows, ガリレオなどの automatic update

13

DDoS

- DDoS 攻撃 (Distributed Denial of Service)
  - 正常なアクセスと同じ手順で、故意に時間のかかる処理などを多発させて過負荷状態を作ってサービスを停止させる
  - 通常のアクセスと区別がつかないため排除できない
  - Internet 向けシステムの過負荷に対する弱さも問題
- 現状
  - 2000年2月Yahoo!, eBay, Amazon.com, CNN.com, Etrade, Microsoft が次々と停止
  - 現在では日常的に行われるようになった
  - 「週に4000回以上」2001.5 カリフォルニア大学

14

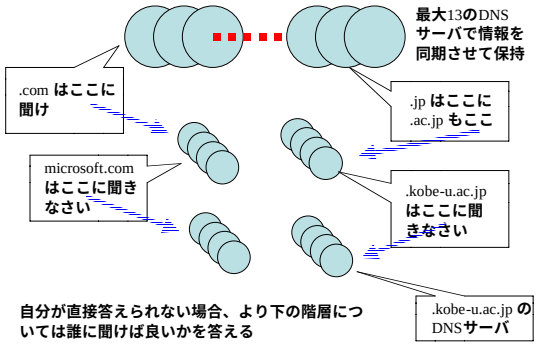
DDoS

- 分散型攻撃が脅威になるということは？
  - そこに集中点があるため
  - 非集中型であるはずの Internet における集中点とは？
- 巨大 Web/mail サーバ
  - Amazon, Hotmail など、従来からのインターネットのキープレイヤーは皆集中巨大サービスタイプ
  - しかしこれらは分散化の可能性もある
- DNS が危ない
  - DNS (Domain Name System)は分散型データベースだが、root 部分は集中型

15

DNSの構造

DNS とは:「この名前のIPアドレスは何か？」と問い合わせるだけの単純なシステム



自分が直接答えられない場合、より下の階層については誰に聞けば良いかを答える

16

DNSの弱点

- Root DNS サーバは最大13 しかない
  - 営利組織、非営利組織、大学、研究機関、NASA、米軍らで運用。10がUS、London、日本、スウェーデンに一つずつ
  - DDoSの攻撃対象になり得る（資料）
  - 2002.9.11 以来、安全性に対する意識がより強くなっている（自由より安全を）
  - 政府介入の可能性
- インターネットのガバナンス
  - グローバルなシステムをどうやって支えていくか、ということに対するグローバルな調整機構などを我々はまだ持っていない

17

犯罪

- ネット社会における Security System の一部
  - 実社会でも同じ：鍵をつけることと犯罪として摘発・処罰するのは対である
  - システムの安全性は高める必要があるが犯罪として定義することも重要
  - 不正アクセス禁止法（H.12.2.13 施行）
- 国内ネット利用者5000万人時代
  - 通常の犯罪がネット上で発生
  - 出会い系サイト、詐欺、etc…
  - 全方位でネット社会を作るという意識が必要