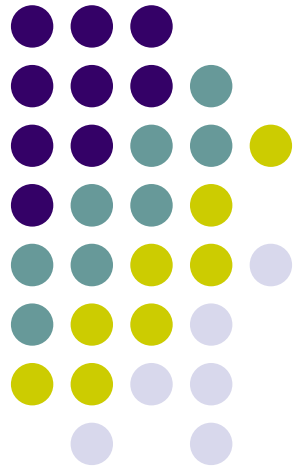
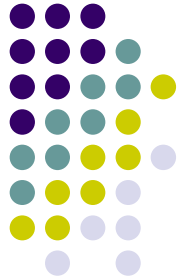
龍谷大学理工学部の中の人から見た、最近のウイルスについての考察

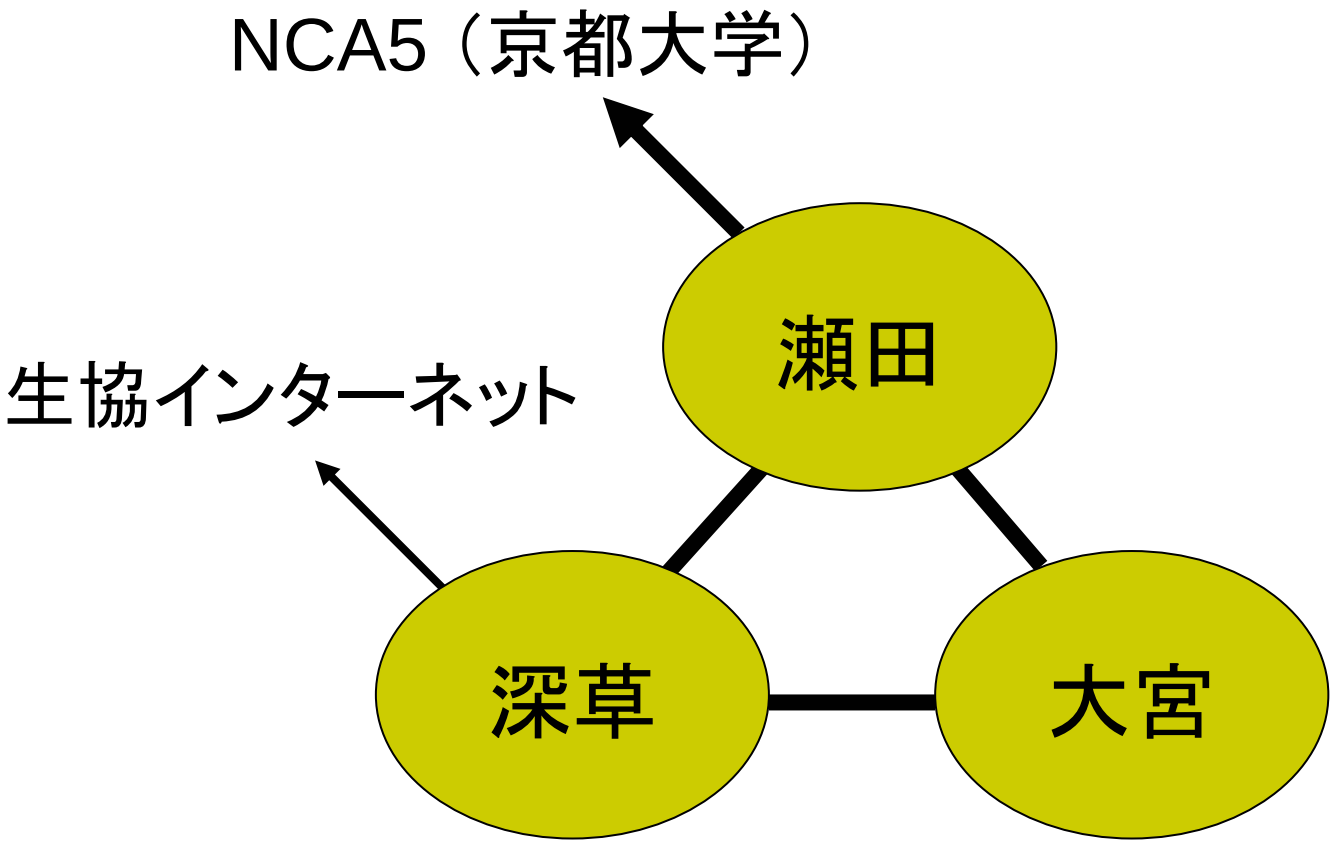
龍谷大学 理工学部
小島 肇



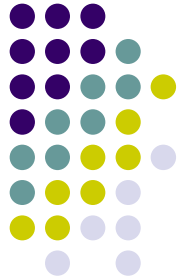


背景となる状況

龍大ネットワーク

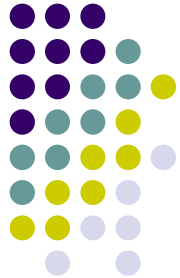


アンチウイルス道具立て



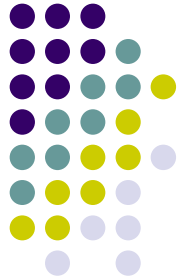
- メール
  - 全学（非理工学部）: トレンドマイクロ + F-Secure
    - トレンドマイクロ InterScan Messaging Security Suite
    - F-Secure アンチウィルス Linux ゲートウェイ
  - 理工学部: ソフォス + ClamAV
    - Sophie（デーモン版 Sophos AntiVirus）
    - ClamAV clamd
    - amavisd-new

アンチウイルス道具立て（つづき）



- Windows デスクトップ、サーバ
  - マカフィー（VirusScan Enterprise 8.0i）
- Macintosh デスクトップ、サーバ
  - マカフィー（Virex）（私が選んだわけではない）
- その他、調査用に Norton（激重）や NOD32（軽い）など

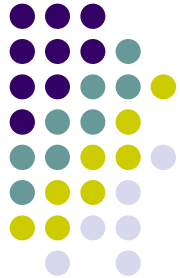
中の人が見ているもの



- 理工学部メールゲートウェイのウイルス状況
- Windows デスクトップのうち、瀬田学舎の教育系に関するウイルス状況
- 自分宛に届くメール
- 各種 web ページ、Mailing List
- 理工学部共通サーバのログ

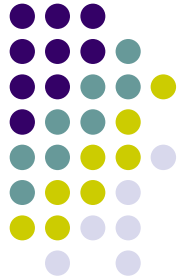
中の人がほとんど見ていないもの

- IDS
- 麻薬系（IRC / IM）
- P2P



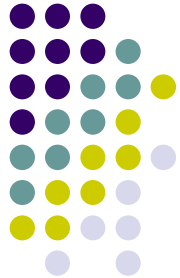
最近気がついたこと

教育系からのウイルス警告が少なくなった



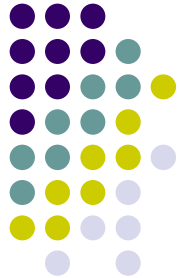
- 主要な無料 web メールがアンチウイルス対応になったためと思われ
  - IE の cache がアンチウイルスに反応する事例が少なくなった
- 持ち込み系が若干増えつつあるか?
  - USB メモリ
- 全体としては大幅減

最初に対応するのは ClamAV（ということもある）



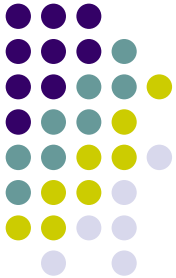
- 最近くりかえし発生した状況
  - ClamAV（だけ）がウイルスを検出。ソフォス、トレンドマイクロ、F-Secure、マカフィー、シマンテックいずれも検出せず
  - しばらくするとソフォスが対応
  - もうしばらくすると F-Secure が対応
  - ……3 大ベンダーは?

3 大ベンダー品の（正規）対応は遅い



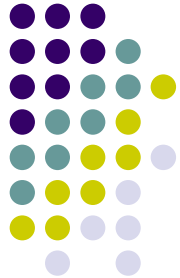
- 緊急対応（ERRATA.DAT、バンデージパターンファイル）でごまかし ← これって結局 at your own risk
- マイナー系アンチウイルスのほうが対応が早い:
  - Kaspersky
  - BitDefender
- シマンテックの対応が特に遅いような気が?
  - F-Secure AntiVirus には Kaspersky のエンジンが搭載されているのだが、Kaspersky 自身よりも対応が遅い気がする

3 大ベンダー品の（正規）対応は遅い



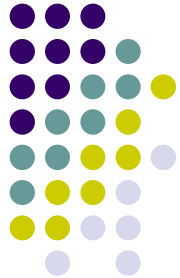
- ウイルス作者はメジャー系アンチウイルスについてはあらかじめ調査した後にウイルスを投下?
- 顧客が多い = 社会的責任も大きい = テストケース膨大 = 対応が遅い?
  - デスクトップ / サーバについては、誤検出があると被害が大きすぎる
  - ゲートウェイについては必ずしもそうではない = マイナーな会社でも ok ？
    - ClamAV は十分使える

ClamAV のおもしろいところ



- フィッシング対応ルールがある。例:
  - HTML.Phishing.Bank-1
  - HTML.Phishing.Action-10
  - HTML.Phishing.Pay-38
- sendmail の milter に対応
  - amavisd-new とかインストールするよりは手軽
- Windows 版もある（常駐はしない）
  - Cygwin ベース

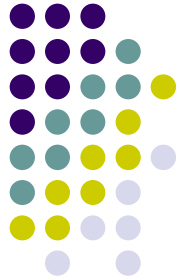
ClamAV のおもしろいところ（続）



- やたらウザいログ

```
Received signal: wake up
ClamAV update process started at Sat Jun 25 03:03:18 2005
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.85.1 Recommended version: 0.86.1
DON'T PANIC! Read http://www.clamav.net/faq.html
main.cvd is up to date (version: 32, sigs: 34720, f-level: 5, builder: tkojm)
daily.cvd is up to date (version: 956, sigs: 1384, f-level: 5, builder: sven)
```

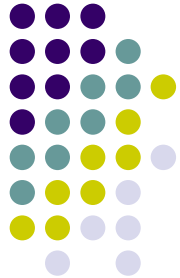
対処できていないところ



- スパイウェアもの

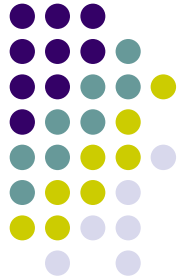
```
% zgrep -i gator.com /var/log/squid/access.log.20050625.gz | ¥
        awk '{print $3}' | sort | uniq |wc -l
    15
```

- でも Gator って VirusScan Enterprise でも対応されていたような（汗）
  - 上記 15 ホストには VSE 入ってない?（滝汗）



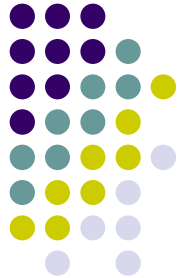
今後の話

Q.ひとはなぜキンタマだの山田だのに感染するのか?



- A. Windows だから
  - 「実行ファイルは実行されるべき」という思想は、いいかげん捨てるべき
    - 実行形式ファイルを IE でふつうにダウンロードすると、いきなり実行許可ビットが立ってしまっているというその思想がだめ
  - デフォルトで自動ログオン・管理者権限
    - 通常利用も管理者権限
  - Mac OS X もデフォルト自動ログオンだけど…
    - 通常利用は一般ユーザ権限
- Longhorn で変わりますか?

ふるまい検出?



- Cisco Security Agent
- Panda TruPrevent
- ホストベース IPS
- どのくらい使えるものなのか要検証