九州大学における セキュリティ対策事例

笠原義晃
九州大学 情報基盤研究開発センター

目次

- 九州大学紹介
- 九州大学のネットワークとその監視
- トラフィック監視による情報収集について
- 学内におけるセキュリティ問題の現状

九州大学紹介

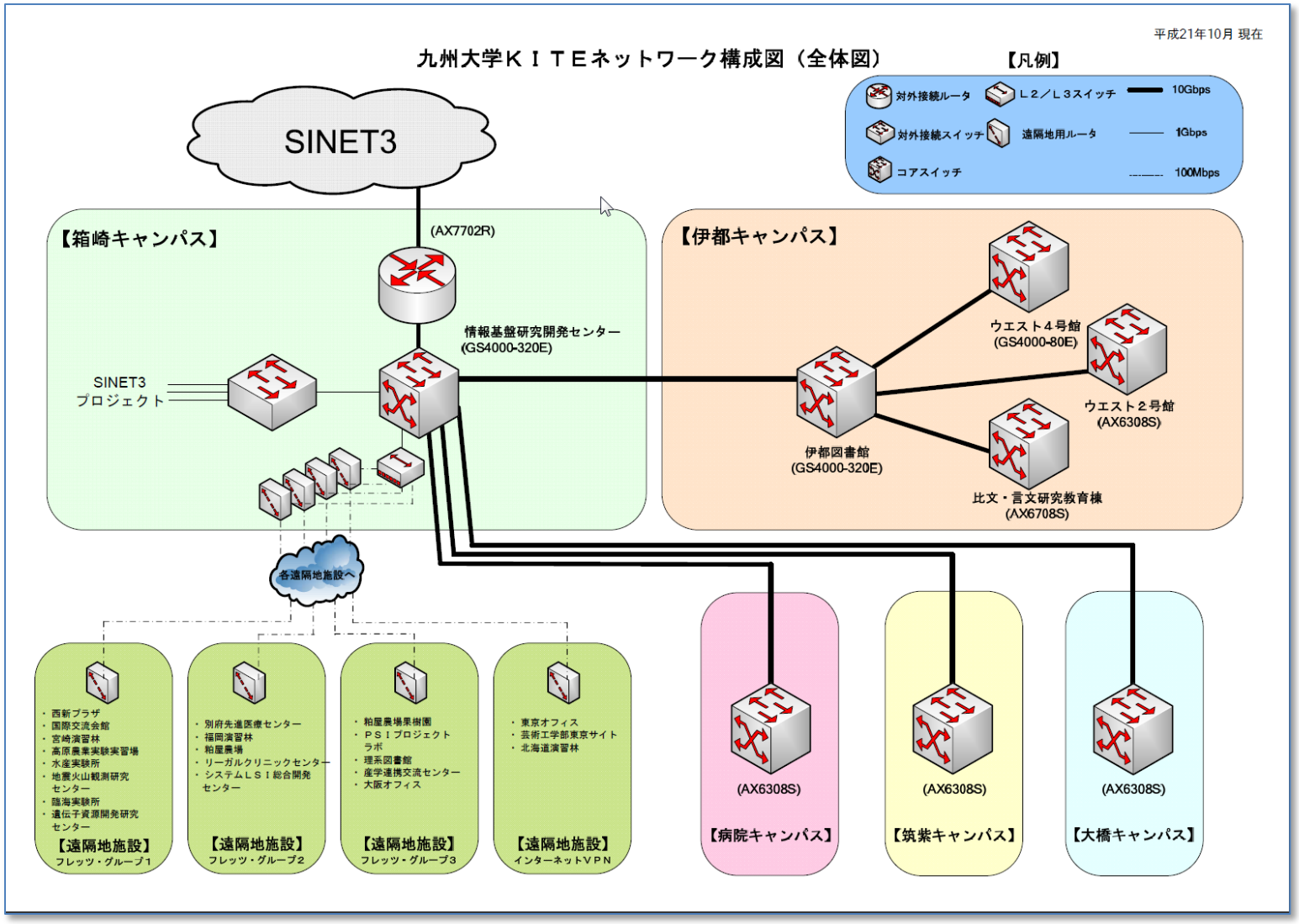
九州大学の場所

（ http://www.kyushu-u.ac.jp/english/university/location/location.php より抜粋）

九州大学キャンパス配置

（http://suisin.jimu.kyushu-u.ac.jp/info/ より抜粋）

ネットワーク構成図


平成21年10月 現在
九州大学ＫＩＴＥネットワーク構成図（全体図）
【凡例】
対外接続ルータ
Ｌ２／Ｌ３スイッチ
10Gbps
対外接続スイッチ
遠隔地用ルータ
1Gbps
コアスイッチ
100Mbps
SINET3
【箱崎キャンパス】
(AX7702R)
情報基盤研究開発センター
(GS4000-320E)
SINET3
プロジェクト
【伊都キャンパス】
ウエスト４号館
(GS4000-80E)
ウエスト２号館
(AX6308S)
伊都図書館
(GS4000-320E)
比文・言文研究教育棟
(AX6708S)
各遠隔地施設へ
・西新プラザ
・国際交流会館
・宮崎演習林
・高原農業実験実習場
・水産実験所
・地震火山観測研究センター
・臨海実験所
・遺伝子資源開発研究センター
【遠隔地施設】
フレッツ・グループ1
・別府先進医療センター
・福岡演習林
・粕屋農場
・リーガルクリニックセンター
・システムＬＳＩ総合開発センター
【遠隔地施設】
フレッツ・グループ2
・粕屋農場果樹園
・ＰＳＩプロジェクトラボ
・理系図書館
・産学連携交流センター
・大阪オフィス
【遠隔地施設】
フレッツ・グループ3
・東京オフィス
・芸術工学部東京サイト
・北海道演習林
【遠隔地施設】
インターネットＶＰＮ
(AX6308S)
【病院キャンパス】
(AX6308S)
【筑紫キャンパス】
(AX6308S)
【大橋キャンパス】

規模

- 5つの主要キャンパス
  - 伊都・箱崎・病院・大橋・筑紫
- 学生 約19,000人
- 教員 約2,200人
- 職員 約2,600人
  - （ http://www.kyushu-u.ac.jp/university/data/index.php より）

情報基盤研究開発センター

- 研究組織かつサービス提供組織
- 情報システム部と連携して各種サービスを提供
  - スーパーコンピュータ等の研究用計算機
  - 教育用計算機
  - 学内ネットワーク
  - キャンパスライセンス
  - 全学共通ID
  - e-Learning
  - ホスティング
  - 全学基本メールサービス
  - etc…

九州大学のネットワークとその監視

キャンパスネットワーク

- 名称: 九州大学総合情報伝達システム
  - KITE: Kyushu University Integrated information Transmission Environment
- クラスBネットワーク 133.5/16 を保有
  - ほぼクラスCサイズに分割し部局単位で管理
    - より小さいサブネットへの分割もあり
  - サブネット数は200程度

ーネットワーク管理者の悩み

- 「ネットワークセキュリティ」
  - 「悪意のあるプログラム」による端末の不正利用、不正アクセス
    - ウィルス等による「被害」
    - ウィルス等による「加害」
    - 不正侵入
    - ウェブページ改ざん（フィッシング）
  - 違法ファイル交換
  - 情報漏洩
  - 等々…

九州大学(固有？)の事情

- 部局ごとの独立性
  - 末端ネットワークは個別管理
- 端末の環境がバラバラ
  - Windows、Macintosh、PC-UNIX
  - UNIX ワークステーション
  - スーパーコンピュータ
- 学生の存在

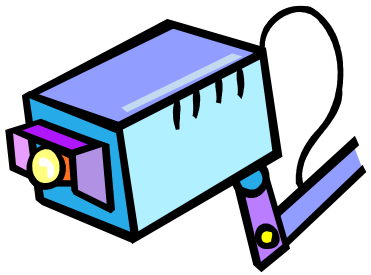
- 各種端末の使い方やセキュリティ対策を強制できない

防御と監視

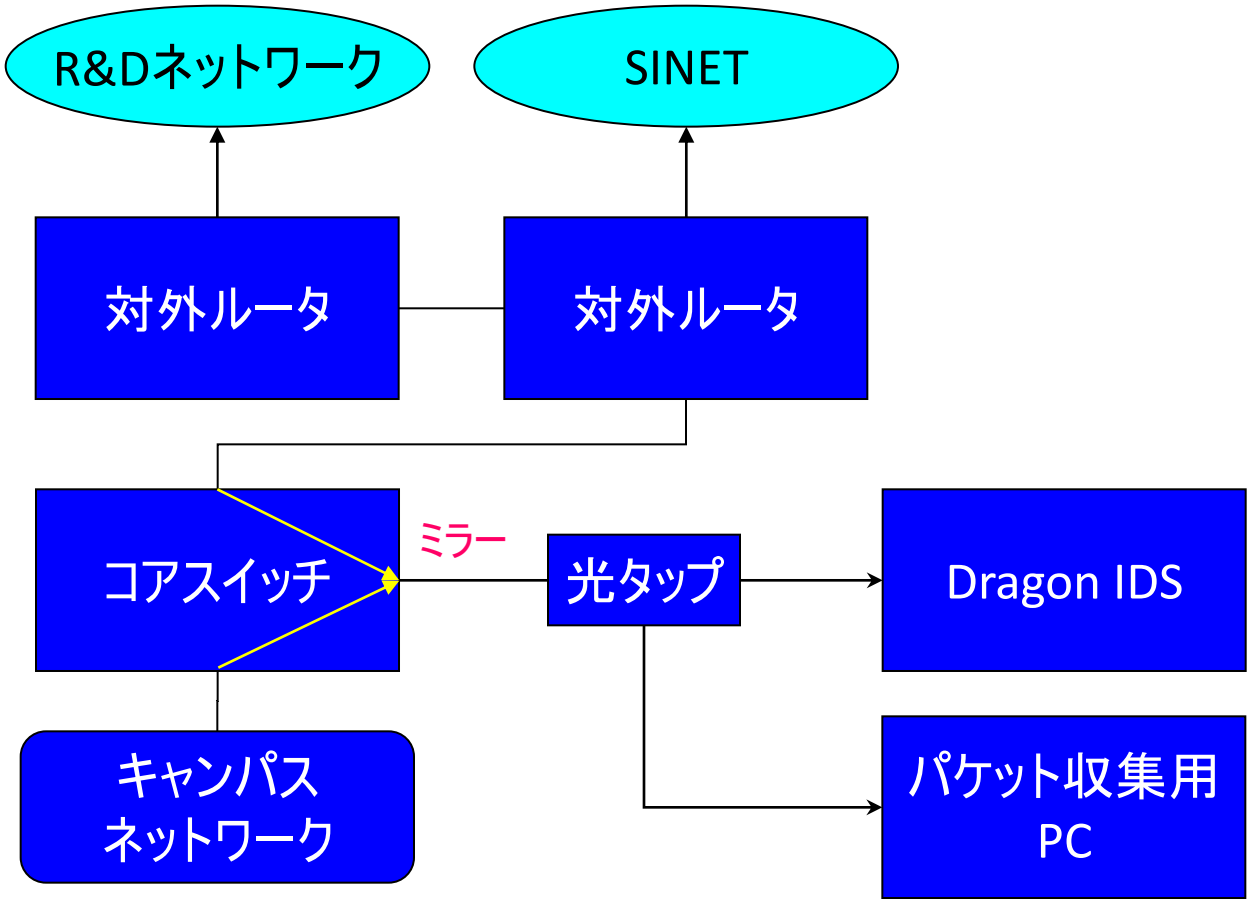
- 本来は予防対策が重要
  - 端末単位で防御するのが理想だが…
    - 対策ソフトのサイトライセンスでの提供等
  - 完全な防御はいずれにしても不可能
- 事後でも早期発見して対応したい
  - 被害の拡大・外への加害を食い止めるため
- 端末での監視は困難
- ネットワークトラフィックを見るしかない？

センターによる監視

- 侵入検知システム（IDS）＋パケット収集PC
  - 学内と学外の間の通信を監視
  - IDSはポートスキャン等にも反応
    - 原因まではわからない
  - 手作りスクリプトで補強
  - 学内同士のやり取りは見えない
- ネットワーク機器監視システム
  - Peregrine Network Discovery
- 外部のP2P監視サービス
  - P2P Finder (CROSSWARP社)



IDS等による監視場所



侵入検知システム

- Enterasys Dragon IDS（商用）
  - http://www.enterasys.com/
  - シグニチャ型ネットワークIDS
- RedHat Linux 上で動作
  - イベントデータベースのフォーマットは公開
  - Perl スクリプトで簡単に扱える
  - 集計処理などが簡単でうれしい ☺
- 2002年11月から稼働中
  - 諸事情によりアップグレードできないまま ☹

パケット収集用 PC

- SuperMicro SuperServer 6022P-i
  - Intel Xeon 2.4GHz (1CPU)
  - 1GB memory
  - PCI-X slots
    - Intel PRO/1000 NIC
    - Adaptec 29329A Ultra320 SCSI
- Newtech Ultimate II SATA RAID
  - 2TB (RAID5)/Ultra160 SCSI
- FreeBSD 6-STABLE
- NetOptics 2x1 regeneration tap 96282-2

パケット収集PCでよく使うツール

- 受動的ツール
  - tcpdump
    - パケット単位での解析の定番
  - ngrep
    - パケットペイロードに対し正規表現検索
  - p0f
    - 受動的にパケット送信OSを推測
- 能動的ツール
  - nmap
    - ポートスキャン・サービス判別ツール
    - 学内攻撃元の種別特定・裏口確認等

トラフィック監視による情報収集

特に注目している通信等

- Internet Relay Chat (IRC)の参加要求
- psyBNC（IRC proxy）のバナー
- ~~HTTPS ポートで走るシェル~~
- 特定のポートへのポートスキャン（SSH等）
- 既知のDDoSツールによる通信
- ~~特定の形式の添付ファイルつきメール~~
- SMTPポートの重点的監視（本文は見ない）

毎日のレポート

- ポートスキャン・ホストスキャン
  - ワーム等の検知
  - IDS内蔵の機能で信頼性は微妙だがないよりマシ
- IRC サーバへの接続状況集計
  - 手作業であやしいサーバを登録して表示
- ~~ウィルスメール検知~~
  - ~~危険な拡張子にマッチしたイベントを集計~~

IRCアクセス監視出力（例）

```
2006Dec08

Outgoing:
? 133.5.[redacted]   - 82.94.222.186       00:03:54-23:35:33     87
! 133.5.[redacted]   - 161.53.178.240      00:22:09-00:48:38      3
! 133.5.[redacted]   - 64.18.128.86        00:22:31-04:08:56   1477
B 133.5.[redacted]   - 85.17.52.79         00:56:36-00:56:38      2
B 133.5.[redacted]   - 80.34.255.4         00:56:53-00:56:53      1
B 133.5.[redacted]   - 85.17.52.79         02:07:28-02:07:28      1
? 133.5.[redacted]   - 220.194.170.5       04:04:14-20:21:15      4
B 133.5.[redacted]   - 80.34.255.4         08:30:44-08:30:44      1
B 133.5.[redacted]   - 80.34.255.4         08:37:16-08:37:16      1
? 133.5.[redacted]   - 220.194.170.5       08:50:13-20:20:04      2
. 133.5.[redacted]   - 192.244.23.4        09:56:22-09:56:22      2
B 133.5.[redacted]   - 80.34.255.4         10:09:30-11:53:17      2
. 133.5.[redacted]   - 192.244.23.4        11:25:22-11:25:22      2
. 133.5.[redacted]   - 219.105.44.202      12:04:41-12:04:41      2
B 133.5.[redacted]   - 80.34.255.4         13:27:00-18:02:35      3
B 133.5.[redacted]   - 80.34.255.4         13:49:29-22:39:43      3
B 133.5.[redacted]   - 80.34.255.4         15:53:32-23:05:29      3
. 133.5.[redacted]   - 192.244.23.1        17:16:14-17:16:14      1
- 133.5.[redacted]   - 211.233.28.196      17:35:28-17:35:28      1
- 133.5.[redacted]   - 211.115.109.27      17:36:07-17:36:07      1
B 133.5.[redacted]   - 80.34.255.4         18:24:44-20:34:29      3
B 133.5.[redacted]   - 80.34.255.4         19:48:50-19:48:50      1
```

SMTPクライアント名監視

- 自分の名前を偽るクライアントを検知

```
Subject: SMTP client name abuse alert
Date: Fri, 23 Oct 2009 12:01:28 +0900 (JST)

2009/10/23 12:01:21.508782 133.5.***.***: 50/1492
xlsqqigdbiigvsvigqvldsdqbinginis
xfapumhkfruckwcupmhwcrufprwfrhwc
xffxksxnpdsussuxdnuifxfpdfpdnxxn
xkhwcuurapcfkhprfrfkahkcrfmucwaw
xsbqgvsblgglsvxdllqxbdsddbnlbvbx
xrfcpruhrprakrwhukmfucmcrrmcwcpc
xglgdsdbnbbdsgvvnlsisngnvqddilxg
xpwcpuwprkkfkcwckhwmrkwupchchprk
xcrrpcfwwfhpawhrpcwcfkrkhppcawff
```

学内におけるセキュリティ問題の現状

Windows 系の被害状況

- ウィルス等への感染
  - 迷惑メール送信
  - ~~感染パケットばらまき~~
  - IRC 接続
    - ボットネットに参加しコマンド待ち
    - ~~IRoffer などでファイル交換用サーバとして~~
- 派手な感染は減っている
- 対策ソフトですぐ駆除できない物が増えている

- スパイウェア等の状況は把握できていない

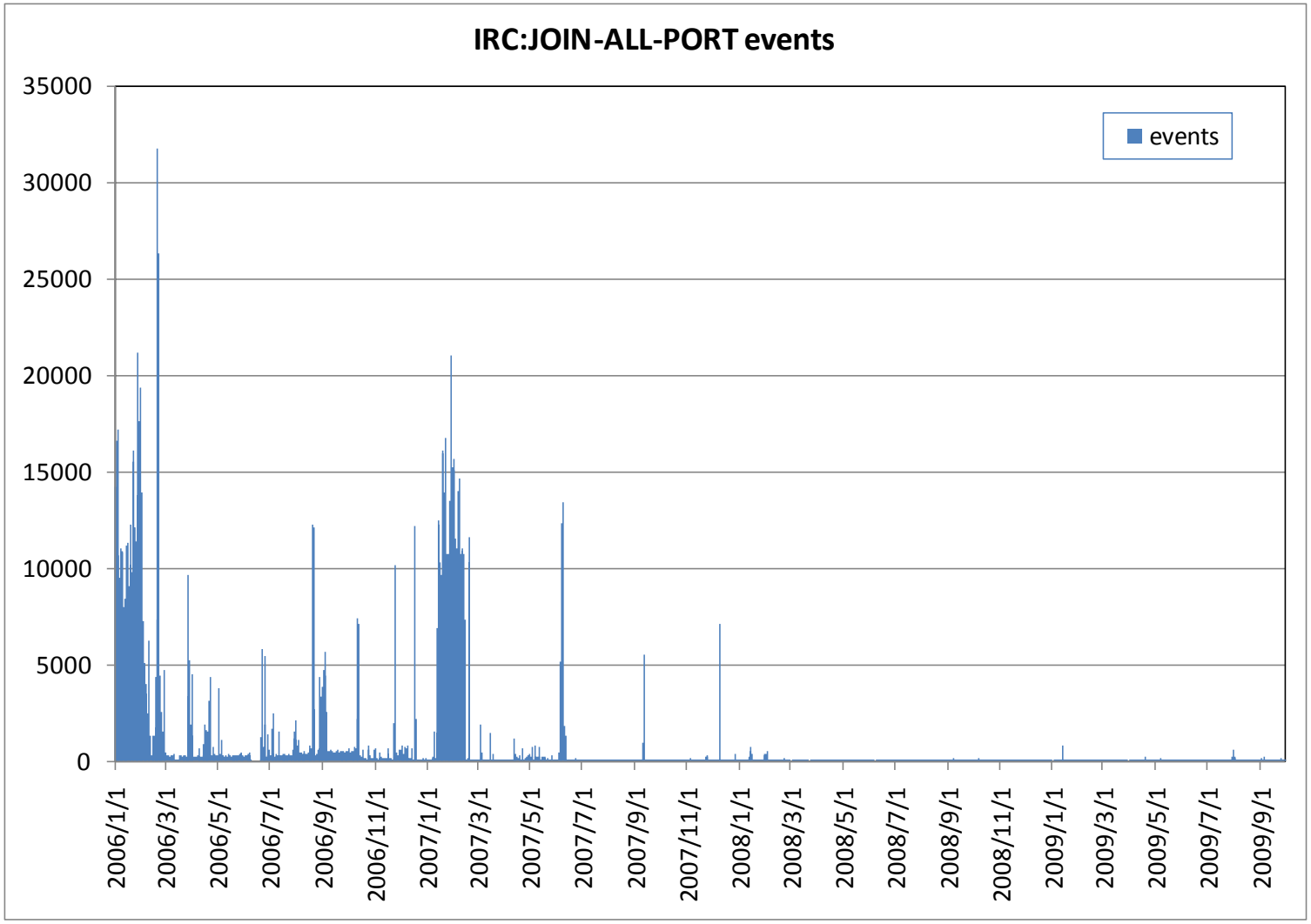
ボット被害（加害？）

- 「ボット」と呼ばれる有害なソフトウェア
  - PC を支配し奴隷化する
  - 感染すると外部サーバに接続し命令を待つ
    - ボット側から接続すればNATの裏でも平気
- 多数のボット PC で構成されたボットネット
  - DoS 攻撃やさらなる感染の拡大に利用
  - 迷惑メール送信等に利用
- 学内にも参加してしまっているPCがある

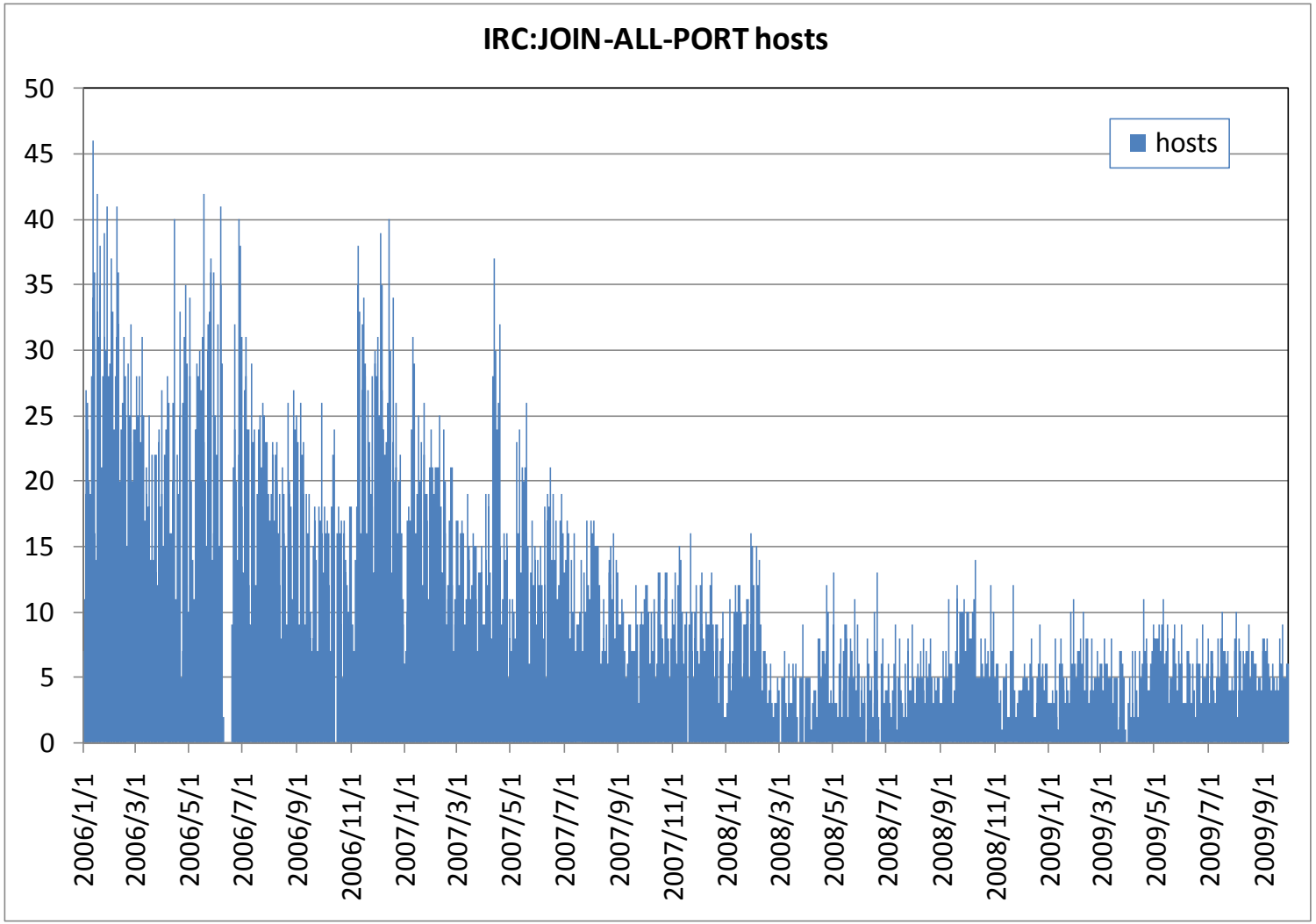
ボットネットとIRC

- ボットへの命令はIRCの利用が主流と言われていた（いる？）
  - 九大に関してはもはやそうでもないようだ
- IRC通信の検知は割と簡単だった
- 独自プロトコルを使われると検知は難しくなる
- 何か別の方法を考えなければ…
  - 模索中

IRC 利用状況（チャンネル参加）



IRC 利用状況（ユニークホスト）



迷惑メール送信

- ウィルス等に感染したPCが、外部からの指令により迷惑メールを送信
- 外部にあるサーバに感染PCから接続に行くため、NATの裏側からでも動く
  - NATの裏からメールが送信されるため、感染PCの特定に手間
- IPアドレスがわかれば、活動中かどうかの検知は簡単
- メールトラフィック全体から活動を検知するのは困難
  - いろいろ模索中

感染経路は？

- 詳しい報告があまりない
  - メールやウェブ経由
  - USBメモリ経由
  - 物理的な端末の移動
- NAT・ファイアウォールの内側でも感染する
  - むしろそういう例が多い気も…
  - 安全だと思って対策を怠っている？
- 突然新種が大発生して数週間で鎮圧
  - だんだん鎮圧までの時間が延びている感触
  - 管理者に通知しても検知・駆除できない→野放し

Unix 系

- 一般アカウントののっとりが目立つ
  - 利用者数の多さから Linux が目立つ
  - SSH を有効にした MacOS X だった、という事も
  - もちろん Solaris でも HP-UX でも同じこと
- セキュリティホールを直接外から踏むものは減少？
  - 巧妙化で気づいていないだけかもしれない

よく見られる攻撃例

- ユーザ名・パスワード総当り攻撃
  - 一般ユーザを乗っ取って悪用
    - SSHが中心だがPOP・FTP等も見られる
  - テスト用アカウント等を破られる事例が多い
- ウェブサーバ等のセキュリティホール利用
  - 減っている感触

- 管理者権限を取られていない事例が増加
  - 他ホストのへ攻撃・プロキシサーバ・フィッシングサイト構築・迷惑メール送信には特権が必要ない

IDS・パケット収集の今後

- 超高速リンクに対するIDSやパケット収集は困難
- 箱崎～他キャンパス間は既に10Gリンク
- SINET3も10Gでやってきた
  - 機材の都合で現状10Gでは監視不能
  - 現在1Gで無理くりミラーしている
- 暗号の普及も障壁になる
- 詳細を知るためにはペイロードも見たいが…
- この方向は厳しいのかな、という悲観的観測
  - できる限りは続けたい

質疑応答