新計算機システム導入とメールシステム統合

~spam対策を中心に~

山形大学学術情報基盤センター

田島靖久

昨年度の話の簡単なまとめ

- Barracuda Spam Firewallを導入して試験
  - BarracudaによるBlack listやベイジアン解析で受信メールの70%を拒否、タグつけで90%を判定
- FortiGateを導入して試験
  - spamを80~90%で検出
- http://www.quark.kj.yamagata-u.ac.jp/~tajima/dpc/report/

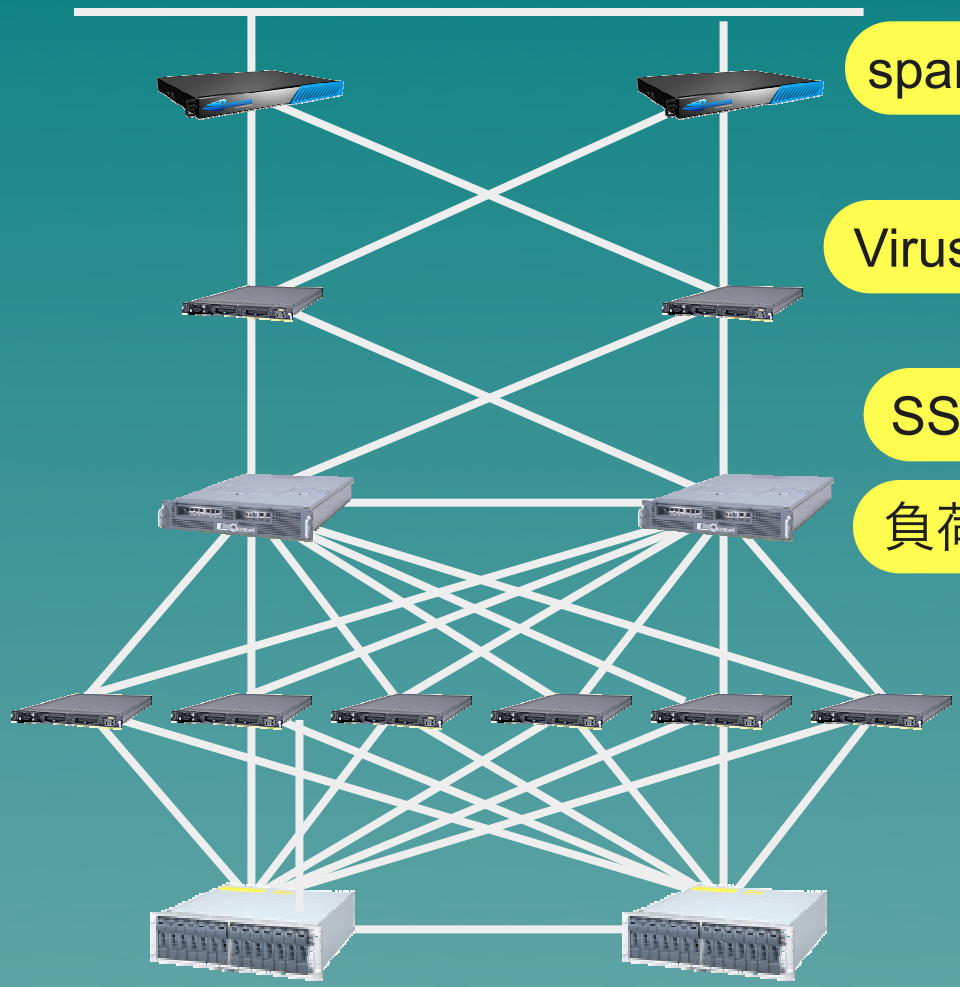
旧計算機システム (~2007.3)

- 4キャンパスにそれぞれ汎用サーバ(Solaris)を設置し、計算兼メールサーバとして運用
  - 計算負荷が高いとメール配送に遅延
  - 個人領域20MB
  - セキュリティのため学内からのログイン or POPのみ許可
- 実習室はWindows2000 ~600台

新システム (2007.4~2012.3)

- 計算サーバとメールサーバを分離
- メールサーバを1台に集約
  - マルチドメイン運用
  - ユーザ領域 1GB
  - WebMail (Active!Mail)の導入
  - POP & SMTP over SSL による学外からの接続サービス
  - Barracuda Spam Firewall によるspam対策
- 実習室はWindowsXP ~700台

メールシステム構成



spam filter　Barracuda Spam Firewall 400

Virus check　InterScan Messaging Security Suite

SSL accelerator　Fujitsu IPCOM S2200

負荷分散　Firewall

SMTP　IMAP

POP　WebMail

Fujitsu Primagy RX200

mail spool (NFS)　Fujitsu NR1000 F270

Barracuda Spam Firewall

- ユーザ数による制限なし
- ユーザ数に依存しないライセンス
- Spam処理
  - ユーザ毎にタグ付け、隔離、拒否が可能(300以上)
- 多言語対応
  - 日本語、中国語他
- 複数メールサーバ対応
- 複数ドメイン対応
- LDAPによるシングルサインオン可能(400以上)
  - http://www.barracudanetworks.com/

（昨年度発表より）

ユーザ情報

- 旧システム
  - 4キャンパスごとにAD domainとUNIX passwd
- 新システム
  - ADをベースにした認証システム
  - 2 domainに集約
    - 工学部は独自サービスをしている都合で別ドメイン運用
  - 2 domain間ではLDAP referralを使って信頼関係を構築
    - 自domainで解決できないときは他方に問い合わせる
  - 配送はADで管理しているvirtual_alias_mapsをメールサーバがLDAPで問い合わせしてアドレスを書き換えて配送

現在の運用(暫定運用)

Barracuda Spam Firewall 1

InterScan Messaging Security Suite

Barracuda Spam Firewall 2

Mail Server x 6

- HA運用、隔離メール用のLDAP認証が未設定のため、IMSSの前後にBarracudaをはさんで運用
  - 試験運用では設定が容易だったためIMSSの下にBarracuda 2 を入れていた。
  - IMSSはメールを受信してから配送するので、戻り先のないspamがspoolに大量に残ってしまい遅延の原因になっていた。Barracuda 1でspamを減らし、IMSSで受信するメールを減らす。

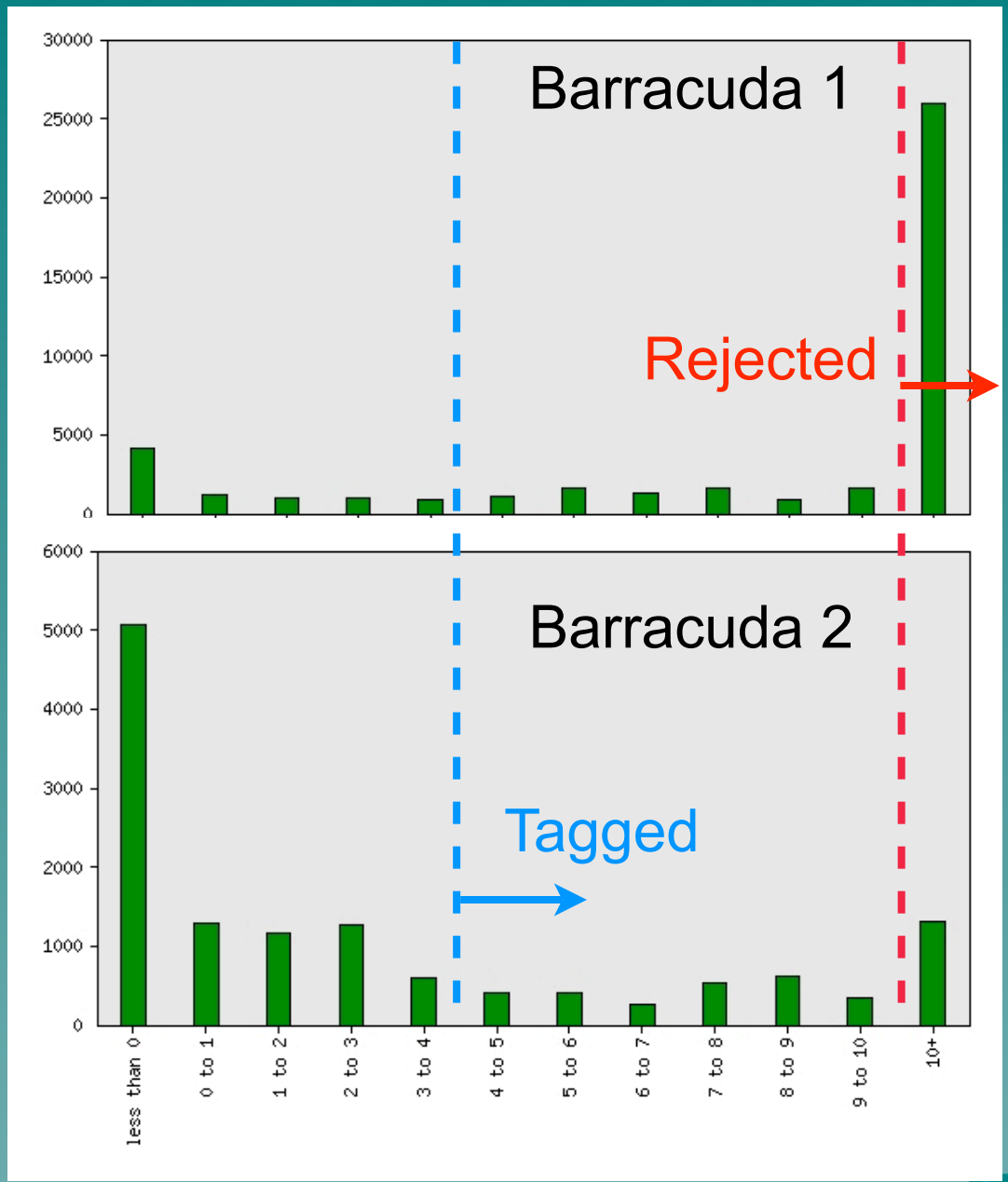
Barracuda Spam Firewall

- firmware upgrade
  - log 検索のインターフェイスが格段に向上
    - 複数keyによる検索の対応、日本語対応
  - Press releaseより
    - Adobe Readerの脆弱性攻撃のブロック
    - 画像spamに対する文字認識エンジン
    - 圧縮ファイルspamに対応
    - real-time protection
- Low end model発売(国内未発売)
  - Barracuda Spam Firewall 100: $899 50名まで。

Spam処理状況

- ~170,000通/day
  - 155,000通 (88%): 受信拒否 (昨年度: 74%)
    - 120,000通 (70%): black-list (barracuda & spamhaus)
    - 35,000通 (18%): spam scoring
  - 8,500通 (5%): タグ付き配送 (昨年度: 9%)
  - 8,500通 (5%): タグなし配送 (昨年度: 17%)

ベイジアンスコアリング



- 2~3くらいのピークは広告メールが多い
- 4を越えるとほぼ100% spam
  - Tagged>4.1,
  - Reject >10
- Barracuda2でスコア10以上のメールはBarracuda1を通らずIMSSに直接配送するメールがあるため。

Anti-Virus Server

- Trendmicro InterScan Messaging Security Suite
- spool問題
  - 一度メールを受信してから内部サーバに配送するため、spamであっても受信してしまう。
    - ユーザ情報をLDAP等で確認できるようなシステムが必要
    - 前段にBarracudaを導入することで特定のホストなどからのspamを受け取らないようにする。

Anti-Virus Server

- 受信者のいないエラーメールの返送先も不在のメールがTTLの時間spoolに残ってしまう。
  - Connection time out
  - Connection refused
  - Host not found
  - 451 VS14-RT5 Mailbox bounce arrival rate exceeds system limit (#4.2.2) xxxxx@yahoo.co.jp
- spoolするメールが増えると遅延が発生
  - 12,000通でI/O waitが発生してperformance低下
  - 100,000通で復旧するために3日間を費やす

Anti-Virus Server

- 添付ファイル問題
  - 10MB以上で隔離
  - 100ファイル以上のzip fileも隔離
    - Office 2007 docx, pptx
      - 実態はxml fileのzip file
      - 場合によっては10ページくらいのpptxでも100file以上
  - コピー機によるPDFファイル生成により、事務からのメールの添付ファイルが急激に増えている
    - ぜひ、コピー会社は圧縮率の高いpdf fileに!

Web Mail

- Active! Mail
  - 複数サーバ、複数ドメイン対応
  - 携帯電話に対応
- Active! Mail 6
  - Ajax を使って利便性をあげる
  - 導入当初は案外不安定で講義での同時アクセスで使えない
  - 最新のupdate (Version6.1)でだいぶ使えるようになる。
- forwardの設定などはWebminを別途導入

おまけ: FortiGate

- 理学部のメールサーバ(ユーザ100名程度)で導入
  - 透過型で運用のためメールサーバの設定変更はなし
  - タグつけのみの運用(理学部の運用ポリシー)
  - SPAM 2466通で2136通(~86.6%)を検知、誤検知は承認広告メール~10通 (先月の個人アカウントでの調査)

おまけ2: Juniper SSG300

- UTMアプライアンス
  - (Firewall/VPN + IDS/IPS + Anti Virus + Anti spam + Web Filtering
    - Anti Virus: Kaspersky Lab
    - Anti spam: Symantec
    - Web filtering: SurfControl

    - Firewall: 450Mbps(320M), 550Mbps(350M)
    - Session: <48,000
    - Interface: 10/100/100Base-T x 4
    - ユーザ数制限なしの様子
- 11/1より日立システムより販売 (10/9 press release)
  - http://www.hitachi-system.co.jp/press/2007/pr071009.html