spam対策

～Barracuda Spam Firewallを使ってみて＋α～

山形大学 学術情報基盤センター

田島靖久

導入の背景

- 事務メールサーバ
  - 広報用に公開しているメールアドレスに、1日100通以上のspamメールが届く
  - セクハラ問題だけでなく業務に影響

センターにspam対策の依頼

spam対策の問題と方針

- 個人ごとに届くメールの種類も違うし、判断基準も違う。
  - 基本的にはクライアントでの対策が一番確実
  - しかし、個人でのspam対策導入はしきいが高い。
- ユーザの意識の問題
  - 導入前:「誤検知で正常なメールが届かなくなってもよい」
  - 導入後:「届かない」「拒否されるのは困る」
- サーバ管理者の意識
  - メールはspamの誤検知もあるので可能な限り配送したい
  - しかしメールサーバの資源(CPU, HDD)への負荷は減らしたい
- 確実にspamと判定されるメールのみ除去し、残りはユーザの判断に任せる

導入機種の選定基準

- アプライアンス製品であること
  - 運用中のシステムに導入するため、トラブル時の影響を最小限に抑える
- ユーザ数（実質）無制限
  - 利用者数が変動してもライセンス金額が定額
- タグ付け、隔離が可能
- 日本語spamに対応
- 本文に対するベイジアン解析によるスコアリングで柔軟な設定が可能

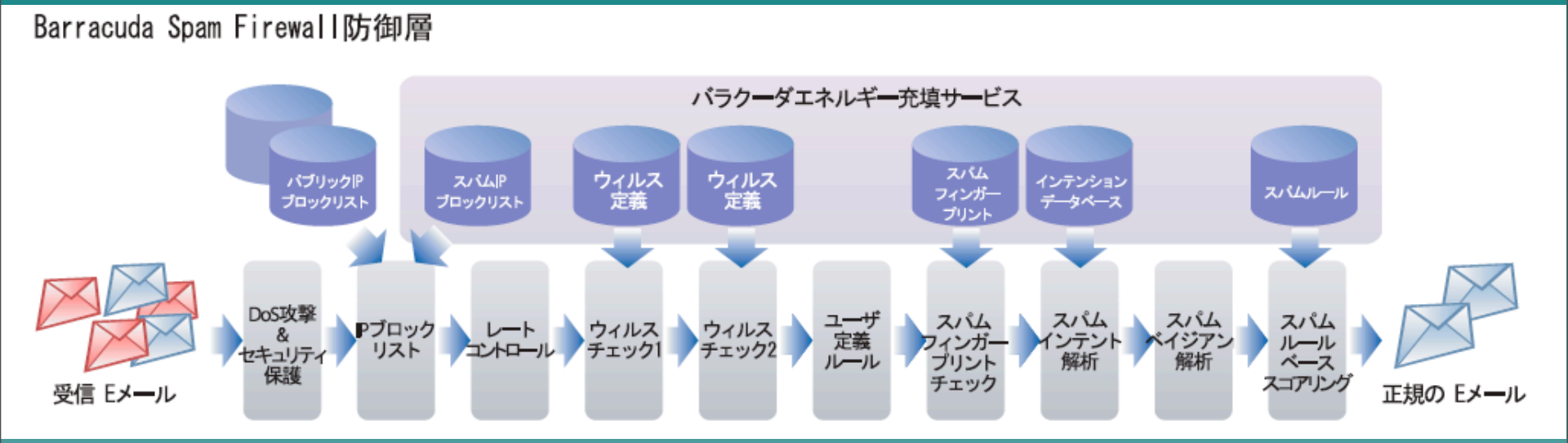
Barracuda Spam Firewall

- 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(400以上)
  - http://www.barracudanetworks.com/

Barracuda Spam Firewall Models

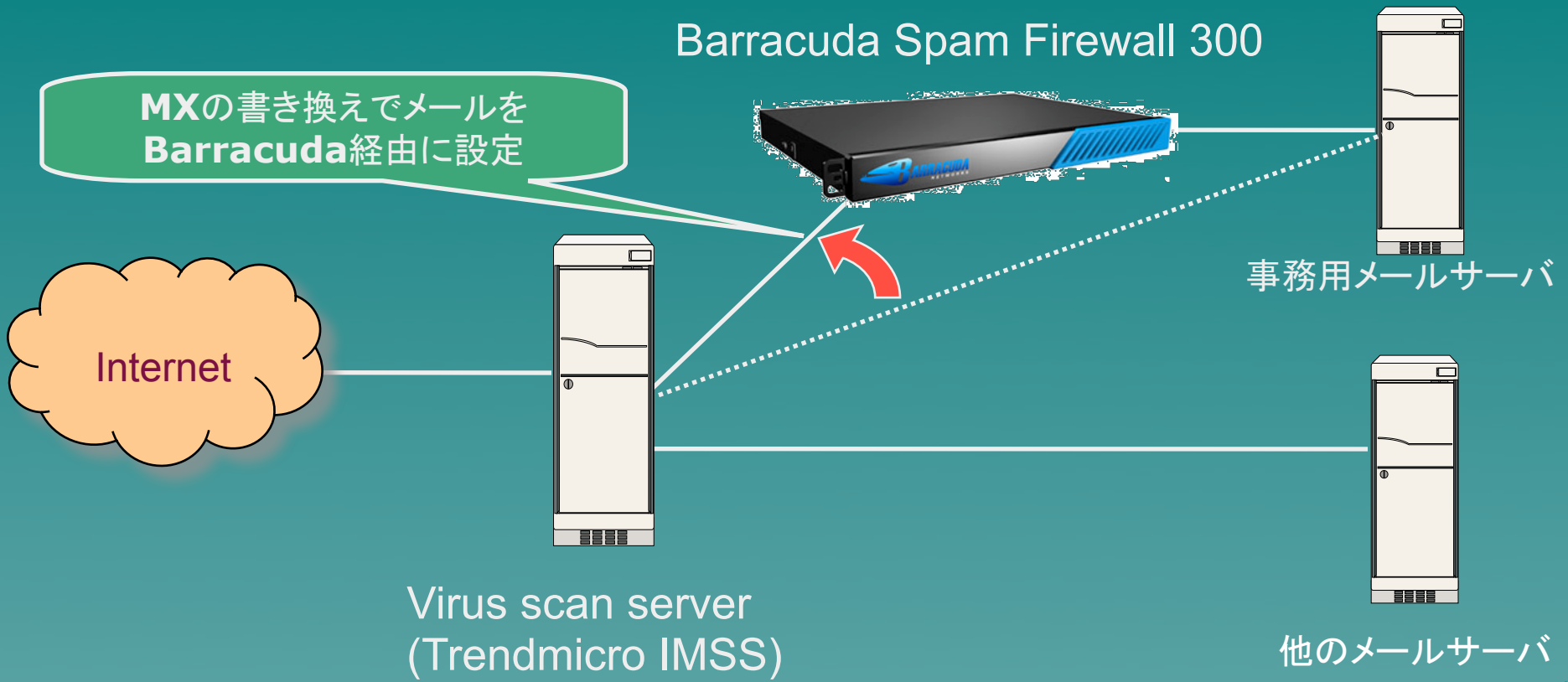
モデル比較	Model 200	Model 300	Model 400	Model 600	Model 800
処理能力*					
一日あたりの電子メール処理能力	100万	200万	500万	1,000万	1,500万
アクティブ電子メールユーザ	1-500	300-1,000	1,000-5,000	3,000-10,000	8,000-22,000
ドメイン	50	250	500	5,000	5,000
隔離保存容量		10 GB	50 GB	100 GB	200 GB
ハードウェア					
ラックマウントシャーシ	1U ミニ	1U ミニ	1U ミニ	1U フルサイズ	2U フルサイズ
寸法（in.）	16.7 x 1.7 x 14	16.7 x 1.7 x 14	16.7 x 1.7 x 14	16.7 x 1.7 x 22.5	16.7 x 3.4 x 26.5
寸法（cm）	42.4 x 4.3 x 35.6	42.4 x 4.3 x 35.6	42.4 x 4.3 x 35.6	42.4 x 4.3 x 57.1	42.4 x 4.3 x 67.3
重量（lbs./kg）	17 / 7.7	17 / 7.7	18 / 8.2	35 / 15.9	50 / 22.7
イーサネット	1 x 10/100	1 x 10/100	1 x 10/100	2 x Gigabit	2 x Gigabit
AC入力電圧（アンペア）	1.0	1.2	1.4	1.8	3.5
冗長ディスクアレイ（RAID）			✓	✓	ホットスワップ
冗長電源					ホットスワップ
特徴					
すべての電子メールサーバとの互換性	✓	✓	✓	✓	✓
安全性の高い強化OS	✓	✓	✓	✓	✓
送信メールフィルタリング	✓	✓	✓	✓	✓
MS Exchange/LDAP Accelerator		✓	✓	✓	✓
ユーザ毎の設定および隔離		✓	✓	✓	✓
Syslogサポート		✓	✓	✓	✓
クラスタリング			✓	✓	✓
ドメイン毎設定			✓	✓	✓
シングルサインオン			✓	✓	✓
SNMP/API			✓	✓	✓
カスタマイズ可能なブランディング				✓	✓
ユーザ毎のスコア設定				✓	✓

Barracuda処理ブロック図



※ Barracuda Spam Firewall Datasheet より

運用構成図

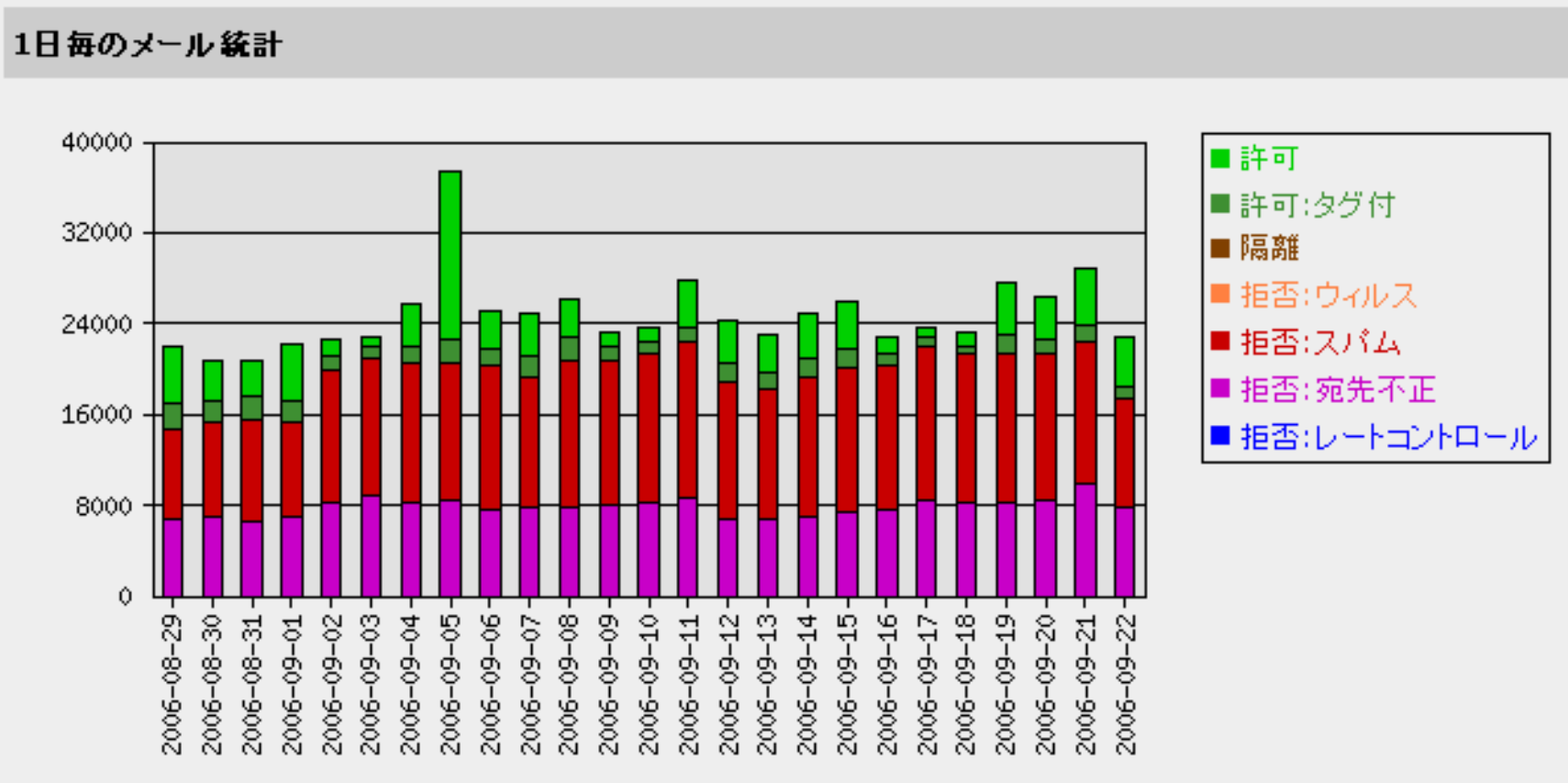


送信者IPアドレスによる判定もあるので、Virus scan serverの前段に設置するのがよいが、今回は試験運用でもありトラブル時にすぐに外せるようVirus scan serverの後段に設置した。

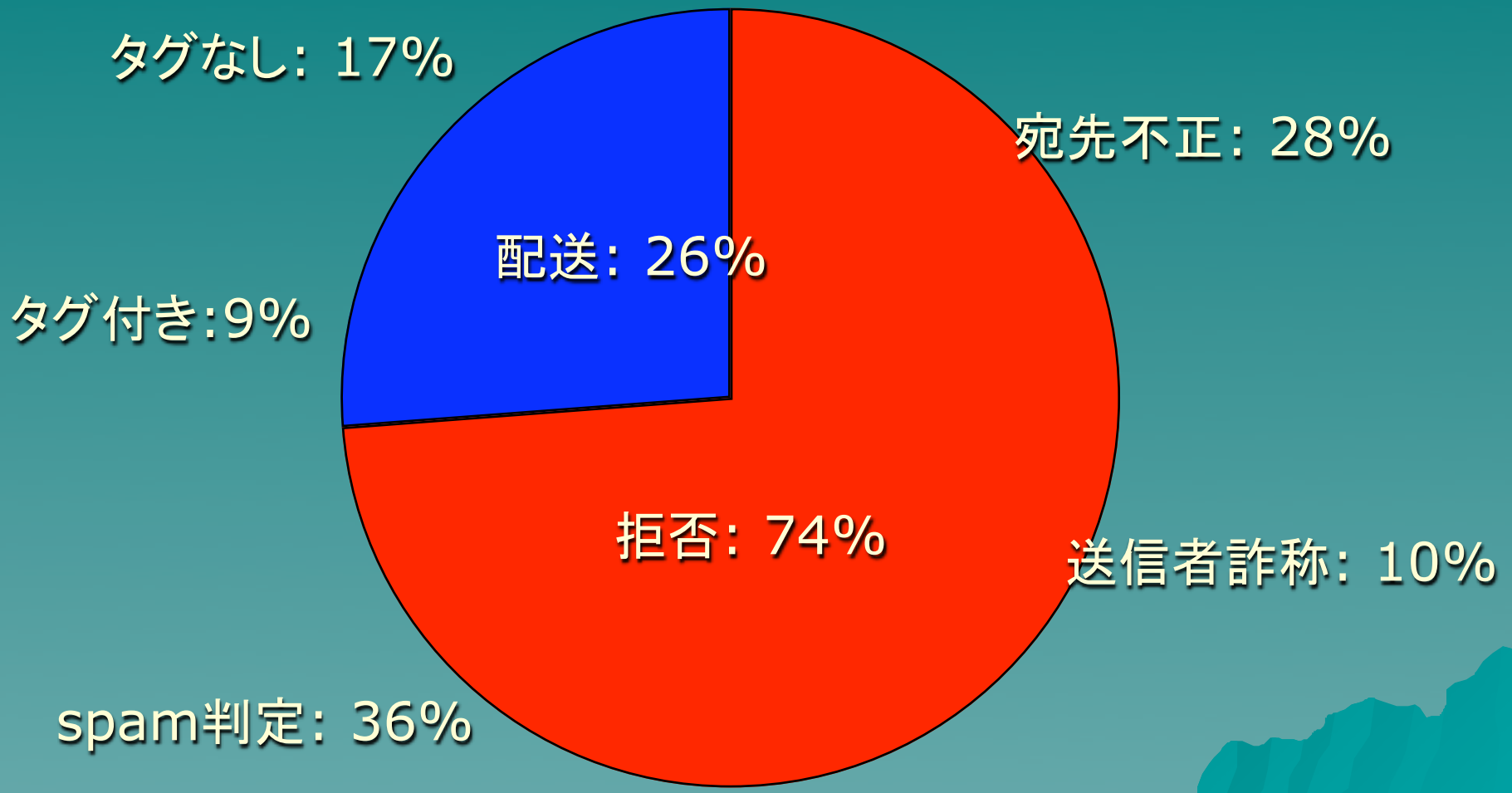
運用方針

- 管理者、ユーザともに手間のかからない運用
  - 確実なspamメールは拒否
    - Source IP Black List
    - Barracuda独自+Spamhaus RBL インテンション解析
  - 隔離設定は行わない
    - 管理を簡単にするためと個人ごとの応対を避けるため
  - タグ付けはきつめに設定
    - Spamでない可能性のメールは配送して利用者が判断
  - ウィルススキャン機能は使用しない
    - Virus scan server (Trendmicro IMSS)があるため

運用統計情報


1日毎のメール統計
40000
32000
24000
16000
8000
0
2006-08-29
2006-08-30
2006-08-31
2006-09-01
2006-09-02
2006-09-03
2006-09-04
2006-09-05
2006-09-06
2006-09-07
2006-09-08
2006-09-09
2006-09-10
2006-09-11
2006-09-12
2006-09-13
2006-09-14
2006-09-15
2006-09-16
2006-09-17
2006-09-18
2006-09-19
2006-09-20
2006-09-21
2006-09-22
許可
許可:タグ付
隔離
拒否:ウィルス
拒否:スパム
拒否:宛先不正
拒否:レートコントロール

2006年7月の統計



運用状況

- メールサーバ (2005年11月より)
  - 事務用サーバ+医学部サーバ(センター管理)
    - 利用者:　　約3300名
    - メール量:　　15,000-25,000通/日
- E-mailによる集計情報を自動報告
- 管理ツール
  - Webによる操作(IE以外でも問題なく利用可能)
  - 配送トラブルの原因究明も管理ツールのログ検索で容易に可能
- headerに詳細情報
  - スコアリングの詳細情報をユーザにも提供
- 配送遅延はほとんどなし

運用トラブル (1)

- 初期設定時の問題
  - ベイジアン解析を有効にするためにはspam, 非spamを100通ずつ初めに学習させる必要がある
  - DNS設定ミスで送信メールをBarracudaに経由させたところ拒否
    - 送信メールがBarracudaを経由しないように設定変更
    - 最新ではoutbound modeで対応しているらしい。
- 運用の問題
  - ドメインごとの管理者を設定できない
    - Admin権限を複数の管理者で共有
    - 次期versionで対応予定らしい
  - 日本語subjectのタグ付けの障害
    - タグを付けるときにiso-2022-jpをbase64エンコードしていたsubjectを、UTF-8に変換してbase64で再エンコードするbug
    - Firmwareのupgradeで対応
    - 日本語関連のbugも積極的に修正してくれる

運用トラブル (2)

- 誤検知の問題
  - 広告メールにタグが付くとユーザから苦情
    - そういうものであると理解してもらうように説明
  - 日本アイソトープ協会(http://www.jrias.or.jp/)のURLが入ったメールが拒否される
    - Spammerが利用しているDNS serverを使っているサイトを拒否するRealtime Intent Analysis機能で拒否動作
    - この機能をoffにすることで対処 （Barracudaでは推奨機能ではなかった)
  - 地元CATV ISPなどからのメールの拒否
    - DHCPで割り当てられていたIPの他の利用者がworm感染でspamhaus RBLに登録。white listに登録で対処
    - 現在でも月に1件くらいのペースで同様のメール拒否が発生している
    - 利用者は拒否の理由の説明で理解してくれる
    - ISPも協力的で、連絡すると早急に対処してくれる

隔離設定

- BarracudaのHDDにユーザ毎のメールの隔離が可能
  - 隔離メールが発生した時点で受信メールアドレスのIDを自動的に作成
  - IDの作成、パスワードはメールで自動送信
  - 隔離連絡メールは1通/1日ごとに配送
  - 日数or容量で自動消去
  - 個人ごとにspamフィルタリングのon/offが可能
  - 個人のベイジアン解析の学習も可能
  - ただし隔離、タグ付けのしきい値設定は変更できない。
    - Model 600以上の機種では可能

まとめ

- Barracuda Spam Firewallを事務用サーバと医学部サーバに2005年11月に導入した。
- 受信拒否、タグ付けの設定で90%以上の確率でspamを判定している。Spam判定で70%以上のメールを受信拒否しているのでメールサーバの負荷(CPU, HDD)が軽減している。

- 2007年2月のシステム更新のメールサーバ(利用者15,000人程度)でも導入予定。

おまけ: FortiGate

- ある学部のメールサーバ(約100人程度)のspam対策について相談をうける
- FortiGate: 統合型アプライアンス(UTM)
  - Firewall+IPS+VPN +WebFiltering+AntiVirus +AntiSPAM
  - 新VersionではWinny(P2P) block機能

FortiGate: 運用構成

- Transparent modeがあるので、そのままメールサーバ(利用者10名程度)の前に設置
- 一週間ほど試験運用

FortiGate: 設定画面

FortiGate: まとめ

- 透過型なので、現在のメールサーバの設定はまったく変える必要がない
- ベイジアン解析がないので学習の必要もない
- spamの検出率は80-90%程度
  - 日本語spamに弱いということもなさそう
- 価格も安いので単体のメールサーバで使用するにはよいかも。