

## 運用経験の共有

---

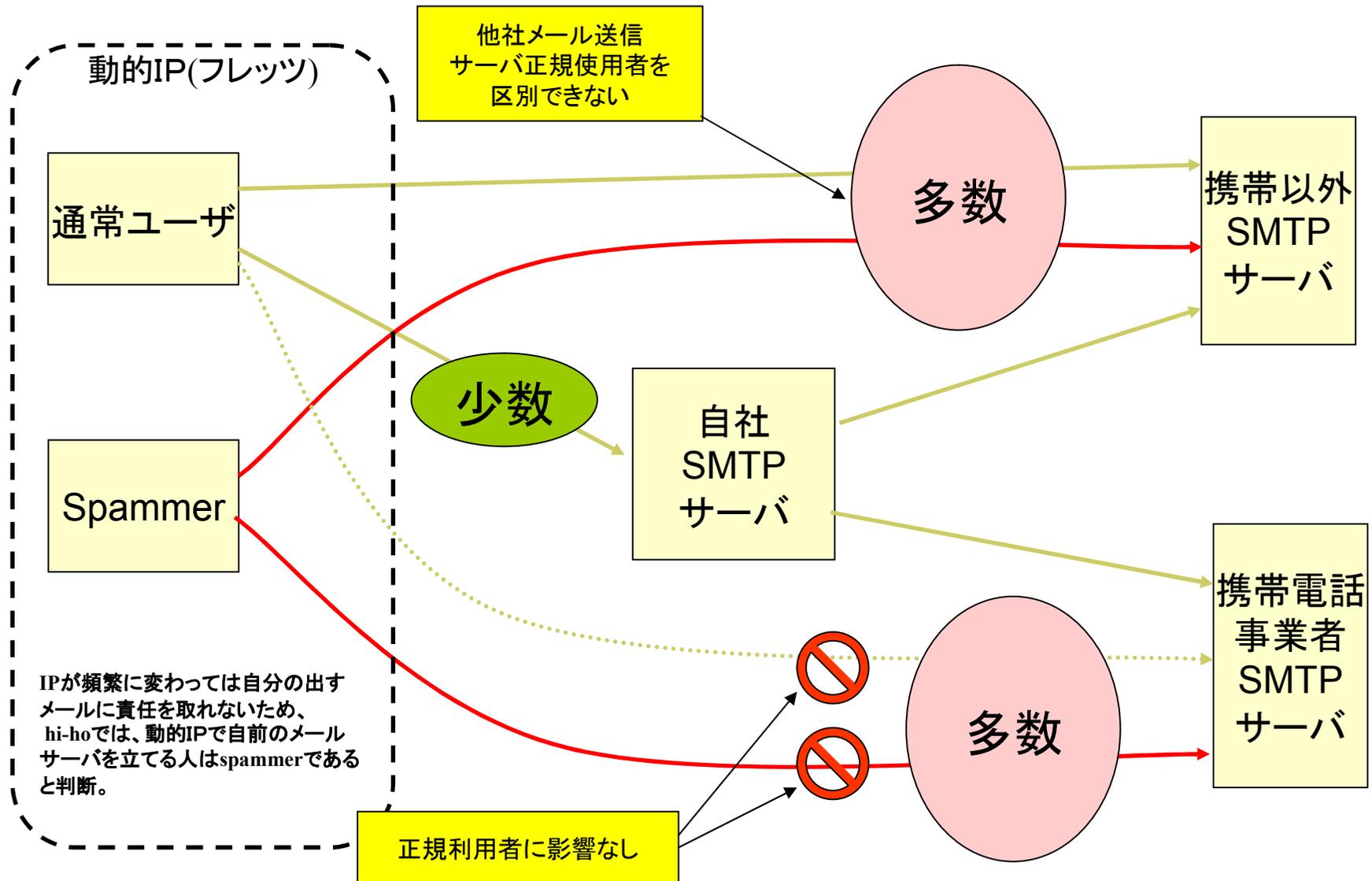
**池田 武** (パナソニック ネットワークサービス株式会社)

- 迷惑メールが動的から多いという仮説をたて、2種類の調査。
- サーバから受信状況を調査
- ネットワークから送信状況を調査

- 2種類の調査。
  - 電気通信事業法により、ISPはお客様の同意がないと実際のメールの内容を調査することはできないため。
- あるメールサーバの約1億通の受信ログに記録された接続元IPを分析。
  - 全メール量は一年で50%増。
  - 固定IPおよび自網内からのメール量は10%増。
  - 動的IPおよび逆引き不可からのメール量は一年で2倍。
  - 日本国内からのメールが大多数を占める。
- ダミーアカウントが受信した約6,000通のメールを分析。
  - 迷惑メールが多数届く私自身の個人アカウントを調査用に提供。
  - 1995年から存在する古いWebページ上にアドレスを晒して収集。
  - **迷惑メールの75%が動的アドレス。20%が逆引き不可。**
  - 動的のほとんどがフレッツ。フレッツを足回りに持つ各社が協調して削減可能。

- フレッツより外部へのトラフィック(パケット数)を調査。
  - 自社サーバ向け……トラフィック少数。
    - 正規利用者がほとんどと推測。
  - 他社サーバ向け……トラフィック多数→即停止不可能。
    - ASPや他ISPのメールサーバ正規利用者がごく少数。
    - 自前サーバによる直接メール送信が多数と推測。
  - 携帯事業者サーバ向け……トラフィック多数→即停止可能。
    - 自前サーバによる直接メール送信が全てと推測。
    - 携帯事業者のサーバはインターネットと携帯の間を中継するものであり、メール送信のために端末のソフトウェアから正規に使用することはありえないことを携帯3社に確認。

# フレッツからのトラフィック調査



- 携帯向けか全体か。
  - 全体を止めると、正規利用者に対する悪影響がある。
    - hi-hoではSubmissionの普及を待つべきと判断。
  - 携帯向けであれば、止めても問題なし。
- どこで止めるか。
  - エッジに近ければ、ルータの負荷は少ないが手数がかかる。
    - hi-hoではこちらを選択。
  - バックボーンであれば、ルータの負荷は多いが手数が少ない。
- 自前サーバの顧客への対応。
  - 中継サーバを使用してもらう方向で対応。
  - 固定IPに移行してもらう。
    - hi-hoは個人向け固定IPのメニューがないため、この選択はなかった。

- 告知をただで流量が半分に。
  - 問い合わせが一日に数件。
  - CS部門からサーバ管理者へのエスカレーションは…。
  
- 実施をすると携帯向けの流量は0に。
  - 予想された効果。
  - お客様からの問い合わせは、CS部門での対応範囲で収まっている。
  
- 携帯以外向けの流量も激減。
  - ブロックを実施した2日後から約1/4に。
  - spammerの傾向として、携帯もそれ以外も同様のツールで送信している？
  - 送信エラーが多くなり、割に合わなくなった？

- OP25Bを全体に広げる
  - 自網外の全てのアドレスに対して。
  - WAKWAKなどが実施済み。
  - @niftyが2006年5月に実施を表明。
  - 2006年度中に対応することを検討中のISP多数。
  - Submissionの推進
- 理想的には
  - 自網内を含む全てのアドレスに対して実施。
  - 解決すべき課題が多いため、長期的視野で検討が必要。
  - 2005年11月現在で、実施済みのISPはない。