インターネットの幸せのために フィルタリングしよう！

2005/01/21 JANOG15@つま恋

株式会社インターネットイニシアティブ
山本　功司 koji@iij.ad.jp

発表のタイトルは「フィルタしよう！」ですが…

- ingress filter はISPとして「本来やるべき filter」
  - というのは合意事項ですよね?
  - でも思ったよりできていないらしい
  - 僕は今ルータを運用してないので ingress filter について何か言うことは難しいのですが
- 一方、ISPとして「本来やるべきではない filter」もある
  - 突発的なincidentは置いておくとして
- 代表的、かつ差し迫った話題としてOutbound Port 25 Blocking について紹介します

Outbound Port 25 Blockingとは

- 動的IPアドレスの回線で外向きの25番ポートへの通信をブロック
  - 自社のSMTPリレーサーバの25番ポートへの通信のみ許可
  - カスタマーエッジに近いルータで行なう
- 動的IPアドレスからのダイレクトなspamやウイルスの発信を防止する目的
- USでは多くのconsumer向けISPで行なわれている
  - AT&T
  - Bell CA
  - Bell South
  - Comcast
  - Earthlink
  - MSN
  - Verizon
  - などなど…

USでの Outbound Port 25 Blocking の実情

- zombie 問題（後述）
- やむにやまれず、ブロックしている
  - spam 発信に対するクレーム処理の負荷
  - 外部からの圧力
  - 動的IPからのspamが多発することにより、IPアドレスレンジ全体（メールサーバを含む）を受信側でブロックされることも
- consumer クラスの回線では port 25 blocking がデフォルトになりつつある
  - 一部ISPではすでに4,5年前から
  - 今年度導入した大手Cable ISPが多い
  - MAAWG でも推奨している

zombie

- Zombie machine
  - Virus等を媒介として、OSの脆弱性をついて PC を乗っ取られる
  - Backdoor が作られ、リモートから制御が可能になっている
  - 最近は大量の zombie machine をまとめてコントロールするネットワークができあがっている
    - Zombie cluster や botnet などと呼ばれる
    - 複数のネットワークの存在
    - 数百台〜数万台（一説によると数十万台とも）のクラスター
- spamの大部分が zombie machine 経由で送られているとの報告
  - Eric Allman のUSENIX2004でのPlenary Sessionによると
    - SPAM全体の90%
    - 少なくとも40%
    - Four fifth(4/5)
    - 資料により差があるが、いずれにしろ大部分と言える
- 一般に、動的IPの先のエンドユーザは素人
  - 管理が不十分
  - パッチ等が適切にあたっていない
  - ユーザの知識が不十分
  - 「zombie にならないように気をつけろ」というのは無理

日本の現状（1）

- USではOutbound Port 25 Blockingが一般的になってきた
  - 日本はどうすべきか、昨年の夏頃から議論
  - MAAWG-J(仮称)や「迷惑メール対策に関する技術交流会」
- 日本では必要ないのではないかという意見が有力かと思われたが
  - 日本ではUSほどspamが深刻ではないのではないか
  - zombieの割合もUSや他のアジア諸国より低いようだ
- 日本もブロックする方向へコンセンサスを作って進むべきだという強い主張をもつ人も少数ながらいるようだ

日本の現状（2）

- 一部のISPでは真剣に実施を検討してきたようだ
  - ISPによって、現状認識に差があった
  - 日本ではISPから携帯向けのspamが多い
  - 昨年夏からzombie経由で日本語のspamが送信されるケースも
- 昨年末、近日中の実施を発表するISPがでてきた
  - ぷららネットワークス
    - 携帯事業者向けに限定
  - WAKWAK
    - 全面的にブロック
  - 追従するISPも出てきそう

日本のメール運用者での議論

- 本来やらなくてすめばそれに越したことはない
- USがやらざるをえない状況であるのは理解できる
- 日本で今やるべきかどうかは意見がわかれる
  - 日本はそこまで深刻な状況ではない
    - フィルタすることにり不利益をこうむるユーザのことを考えると踏み切れない
- いつまでもエンドユーザに自由と責任をセットで押し付けていていいのか
  - 大多数のエンドユーザはtransparentな接続を欲しているわけではない
  - デフォルトで守られたサービスを検討すべき？

ISPだけが悩まなければいけない問題なのか

- Outbound Port 25 Blocking は ISP でないとできないか？
- エンドユーザに近いところでのフィルタの必要性
  - いわゆるブロードバンドルータがその役目を果たせるのでは？
  - ISPの設定情報との連携の可能性
  - Personal Firewall?
- 「ブロックしろ」「ブロックするな」とISPに言うだけでなく、どうすれば問題を解決できるのか一緒に考えてほしい
  - ブロックするにも、いろいろな地ならしが必要
  - ブロックしたくないなら代案を！
    - 日本でもいずれ放置できないレベルに