Gifu Univ
Computer Center

ＳＰＡＭ対策／管理対策

原山　美知子
harayama@cc.gifu-u.ac.jp

岐阜大学総合情報処理センター

Gifu Univ
Computer Center

SPAMについて

•米国では社会問題になっておりスパム対策が進んでいる 次のターゲットは？

America Online（AOL）は米国12月21日，ジャンクメールを配布するスパムベンダーに対して起こしている訴訟で6件について勝訴. 5つの州で新たに9件のスパム訴訟を起こした。これによりAOLは，同社顧客に対する詐欺まがいの広告や，ポルノ広告の配布を根絶やしにする考えだ。

•オープンリレイは必要か？

他のサーバのメール送信を助ける, 送信ルートのテストなどに利用
現在はオープンリレイによるメリットよりスパムの弊害の方が大きいので全面的に止めるべきだという考えが普通.

IPAのセキュリティのページ
http://www.ipa.go.jp/security/ciadr/antirelay.html
Mail Abuse Prevention System (MAPS), California nonprofit company のページ
http://www.mail-abuse.org/tsi/ar-what.html

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

SPAM対策

- 不要なsendmailを止める.
- オープンリレーを止める.
- メール濫用予防システム（MAPS RBL）を利用した，メール中継の拒絶.
- sendmailのバージョンアップ
  - －sendmail 8.9からリレイを止める設定ができる。
  - －最新版：sendmail 8.10.2（ID,Password認証可能）
    ちなみに，Beta版は sendmail 8.11.0.Beta3
  - －CFのバージョン（CF3.7pl2推奨）にも注意.
- POPbeforeSMTPの利用

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

SPAM対策 –MAPS RBL利用例–

gumailのsendmail.cf抜粋

```
SCheck_reject
# deny with MAPS (Mail Abuse Protection System) RBL (Realtime Blackhole List)
# by Paul Vixie
R$*                     $: $1 $| $&{client_addr}
R$* $| 0                $: $1                           command line is OK
#R$* $| $={MapsSkipIP}$*        $: $1                   no checking
R$* $| $-.$-.$-.$-      $: $1 $| $(host $5.$4.$3.$2.rbl.maps.vix.com. $: OK $)
R$* $| OK               $: $1                           fall through
R$* $| $+               $#error $@ 5.7.1 $: "550 Mail from " $&{client_addr} " r
efused, see http://maps.vix.com/rbl"
R$* $|                  $: $1
```


All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

オープンリレイの現状

ドメイ	ORBS登録※	ホスト数	ホスト数※に占める割
全	125,011	72,398,092	0.17%
jpドメイ	11,486	2,636,541	0.44%
ac.jpドメイ	1,676	558,692	0.30%

参照 URL

※1 ORBS Open Relay Behaviour-modification System
Database Dumps (http://www.orbs.org/database.html)

※2 Internet Software Consortium
Internet Domain Survey (http://www.isc.org/ds/)

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

SPAM対策に関するRFC

Network Working Group　　G. Lindberg
Request for Comments: 2505　　Chalmers University of Technology
BCP: 30　　February 1999
Category: Best Current Practice

Anti-Spam Recommendations for SMTP MTAs

Abstractから, 抜粋

A brief summary of this memo is:

- Stop unauthorized mail relaying.
- Spammers then have to operate in the open; deal with them.
- Design a mail system that can handle spam.

本文から, 抜粋

2.1. Restricting unauthorized Mail Relay usage

Unauthorized usage of a host as Mail Relay means theft of the relay's resources and puts the relay owner's reputation at risk. It also makes it impossible to filter out or block spam without at the same time blocking legitimate mail.

Therefore, the MTA MUST be able to control/refuse such Relay usage.

URL => http://www.rfc-editor.org/rfc/rfc2505.txt

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

SPAM対策管理

ORBS，VIXのデータベースやMAPS(Mail Abuse Prevention System) RBL (Realtime Blackhole List)の利用．

ORBS（http://www.orbs.org） VIX（http://www.vix.com/）

ポートスキャンによる学内サーバの調査・管理

学内ネットワーク管理者に対しセキュリティ関連情報提供．

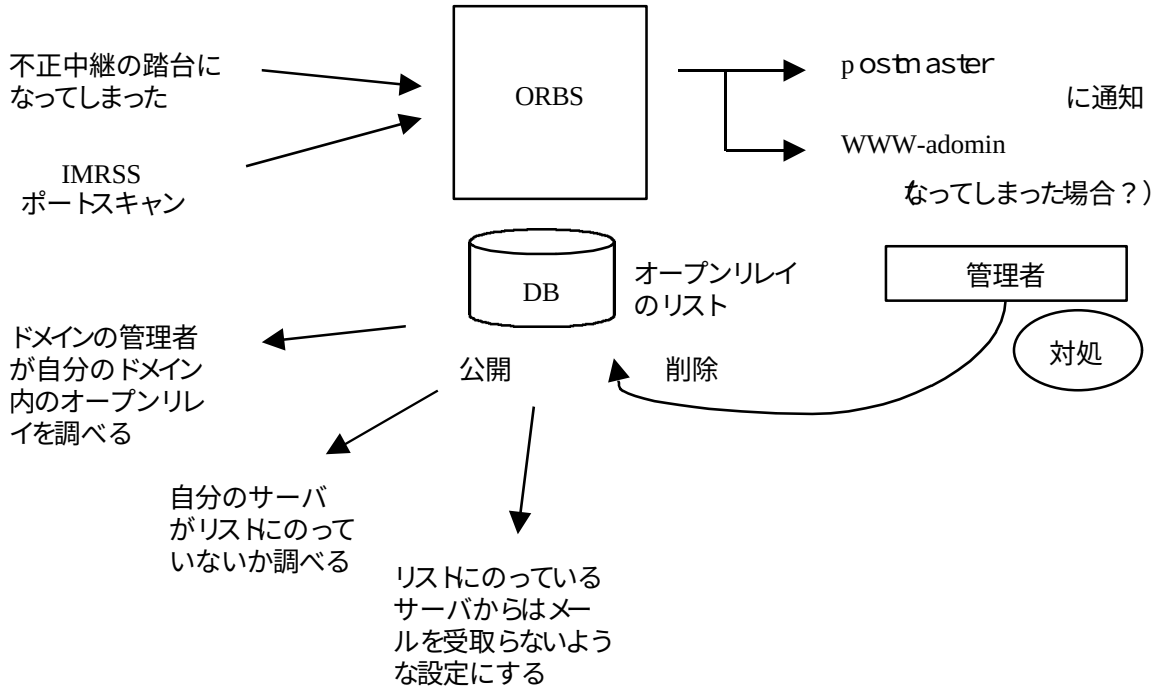
All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

ORBSのしくみ

ORBS ： Open Relay Behaviour-modification System

http://www.orbs.org/



All Rights Reserved, Copyright Gifu Univ. Computer Center

岐阜大学の事例
ー方法１　ORBSの利用ー

1.ORBSからドメインのレポートをとりよせる.

CIDR 形式でネットブロックを指定
133.66
133.66.4/22

admin@orbs.org宛に
単なるダンプか定期ダンプを指定して送る.

2. ORBSから来たレポートに掲載されている管理者に送る.

管理者向けページ
http://www.orbs.org/admins.html

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

ORBSからの通知

To: postmaster@gumail.cc.gifu-u.ac.jp, postmaster@gumail.cc.gifu-u.ac.jp
From: The Open Relay Behaviour-modification System <listings@orbs.org>
Reply-To: ORBS listings <listings@orbs.org>
Subject: Network security problem: 133.66.1.11 is an open email relay
X-UIDL: 7e8e3a3482529cab924b474d49d534f4

Please read this entire message carefully before replying

If you are not the technical contact for your organisation, please
forward this to the person who is.

133.66.1.11 has been detected as an open email relay and has been added
to the ORBS database.

An open email relay is a SMTP server that accepts E-mail from anywhere
on the Internet and forwards it to anywhere else on the Internet

Someone nominated 133.66.1.11 for testing, probably because they
received unwanted junkmail which was delivered via the server.
Inspection of your mailserver logs will reveal more information.

ORBS (http://www.orbs.org) has confirmed this by sending an automated
test message through 133.66.1.11. Delivery of that message back to the
testing program has triggered this warning message.

.
.
.

Thank you for your attention to this matter.
Sincerely,
listings@orbs.org

From: database@orbs.org
Subject: Orbs Database dump 2000-06-26

.
.
.

Entries more than 4 weeks old are automatically retested,
however please file these closed if they've been secured, as the
retesting cycle on hosts previously known open takes at least
2 weeks.

OUTPUT_IP	INPUT_IP	LAST_VERIFIED(UTC)	DISCOVERED
Netblock = 133.66.			
133.66.132.154	133.66.132.154	2000-06-08 - 11:33:39	2000-05-03
133.66.136.49	133.66.136.49	2000-06-19 - 17:12:46	2000-03-18
133.66.137.125	133.66.137.125	2000-06-12 - 08:51:49	2000-03-08
133.66.159.160	133.66.159.160	2000-06-23 - 10:51:19	2000-03-18
133.66.159.193	133.66.159.193	2000-06-23 - 10:50:24	2000-04-25
133.66.161.111	133.66.161.111	2000-06-23 - 10:51:59	2000-04-17
133.66.161.124	133.66.161.124	2000-06-14 - 03:56:43	2000-03-15
133.66.201.61	133.66.201.61	2000-06-19 - 00:41:04	2000-03-19
133.66.38.39	133.66.38.39	2000-06-09 - 03:21:46	2000-04-21
133.66.90.250	133.66.90.250	2000-05-23 - 03:55:05	2000-03-10
¥-<--	133.66.95.254	2000-06-06 - 07:24:39	2000-03-09

All Rights Reserved, Copyright Gifu Univ. Computer Center

学内通知の例

○○○先生

いつもお世話になっています．133.66.132.154のサーバはスパムメールの踏み台となる可能性があります．

こちらで確認したところ，SMTPの設定が不特定の相手にメールのリレーを許す設定になっていました．この設定は，非常に問題ですので，至急ご対応をお願いいたします．

また，上記サーバは，スパムメール・ブラックリスト(http://www.orbs.org/)に登録されています．対応後は，このブラックリストからの削除も行って下さい．お忙しいところ，お手数をおかけいたしますが，大至急ご対応をお願いいたします．

○○○先生

SPAM Mail関連のご対応に関してありがとうございます．まだ，ORBSのリストに残っているサーバがありますので，対応後早急に，ORBSのデータベースからご担当サーバの削除をお願いいたします．お忙しいところ，ご迷惑をおかけいたしますがよろしくお願いいたします．

ORBSのデータベースからの削除の方法

~~~~~~

1. http://www.orbs.org/closed_1.html　のページにアクセスして下さい．．
2. Report a closed relayページが表示されます．
   Please enter the IP address of your fixed relayと書かれた下に，IPアドレスを記入箇所がありますので，そこに削除するサーバのIPアドレスを記入して，[NEXT >>]ボタンを押して下さい．
3. Database Check ページが表示されます．
   そのページの下の方に，[Yes, these have all been fixed]と書かれたボタンを押して下さい．
4. Closed Relay ページが表示され，Thanks! 133.66.xxx.xxx has been removed from our open relay database. の表示が出れば削除OKです．

All Rights Reserved, Copyright　Gifu Univ. Computer Center
~~~~~~

Gifu Univ
Computer Center

効果など

サーバ**管理の問題**
- セキュリティ情報を見過ごしてしまうことがある.
- 一般的な注意情報では、緊急性が不明.

postmaster宛にくるORBSからの通知を見過ごしてしまうことがある。
DNSに登録がされていない場合がある.

ORBSリスト配布に対する学内の対応状況
- オープンリレイを止める.（sendmailの設定を変更する、バージョンアップ）
- 不要なsendmailを停止する.
- 起動時にsendmailが起動しないようにする。
- 不要なサーバ自体を停止する.

この方法のよい点と悪い点
- 学内管理者が早く対応してくれる.
- ORBSのリストに掲載されるまでに, SPAM中継をされてしまう可能性がある.

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

岐阜大学の事例
ー方法２　ポートスキャンー

1. 予め, ポートスキャンすることを予告する
2. ポートスキャンしてオープンリレイを発見する
3. 管理者に通知する

この方法のよい点悪い点

•予防的に対策できる.

•ポートスキャンの意味がわからない管理者には意味がない.

•ポートスキャンに対して反発がある.

•管理体制がきちんとできている部局でないとできない.

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

学内通知の例

コンピュータ管理者の皆様，教官の皆様：

メールの不正中継を行なっているホストがまだあるようです．

応用情報学科が管理するすべてのホスト（IPアドレス）について，メール送信を行っているホストを探します．ポートスキャンという手法を使います．クラッキングでよく使われる方法ですが，今回は管理という意味で使います．Firewall, tcpwrapperなど導入されている研究室では，変なlogが残ると思いますがよろしくご理解下さい．

スキャンを行う元のホストは〇〇研の中のホストです．
133.66.200.*のIPがつきます．

結果を別途報告しますので，不要なメールサーバは停止していただきますようお願いします．

All Rights Reserved, Copyright Gifu Univ. Computer Center

Gifu Univ
Computer Center

使用ソフトなど

•使用ソフト
AGNetTools
（Macintosh版を使用しましたがWindows版もあります）

•AGNetTools の機能
Ping:　Trace Route:　Name Lookup:　Finger:　Whois:　Throughput Tool:
Name Scan:　Port Scan:　Ping Scan:　Service Scan

•参照URL
http://www.aggroup.com/products/agnettools

All Rights Reserved, Copyright　Gifu Univ. Computer Center