Outbound Port 25 Blocking
最近のメール事情

2006/1/28,29

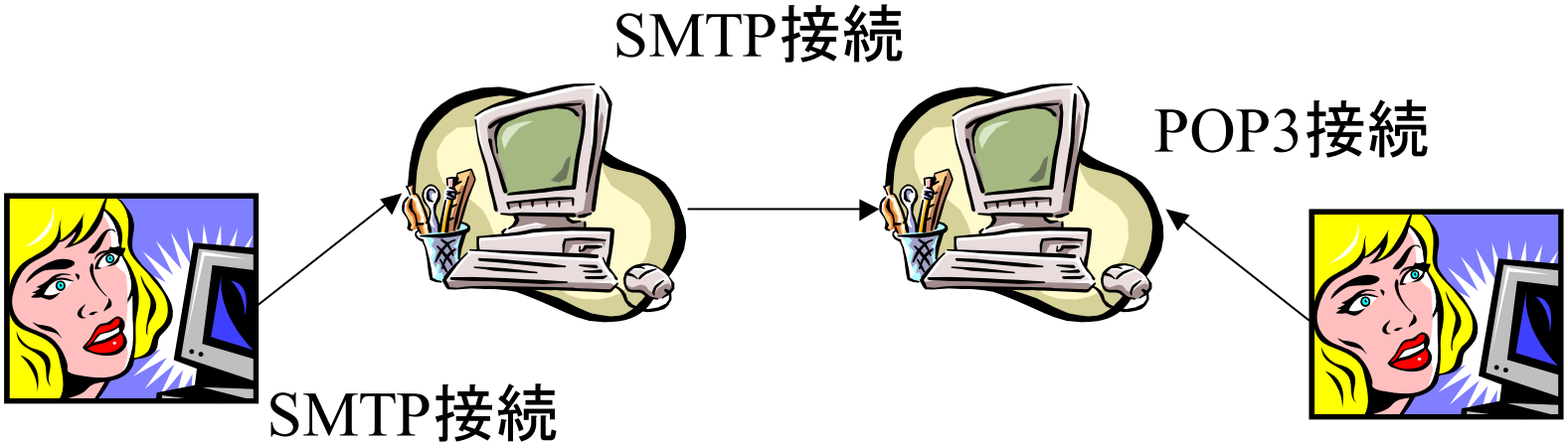
新潟インターネット研究会 神保道夫

karl@nisoc.or.jp

目的

- 最近話題になっている、Outbound Port 25 Blockingについて、その背景と仕組みを知るとともに、サーバー側での実現技術を知ることにより、今後のメールの利用に対する知識を深める。

電子メールの送受信の仕組み



電子メールの歴史(1)

- 日本で一般向けにインターネットサービスが普及し始めた頃(～1997年頃まで)
  SMTPサーバーは、どのサイトからどのサーバーに対しても自由に利用ができた(いわゆるopen relay状態)
- インターネットの普及期(1998年前後～)
  SPAMメールが出始め、open relay状態のサーバーは自サイトのみ接続可となる傾向になる。

電子メールの歴史(2)

- ブロードバンド普及期(2000年頃～)
  SPAMメール:
  (1) 携帯や無料アカウントからの大量投稿
  (2) ウイルス感染によるゾンビマシンが、ADSL、FTTH経由で大量にSPAMをばら撒く

SPAMメール対策(1)

- 今まで自由にメールサーバーを使っていた人にとっては、「メールサーバーが使えなくなるというのは困る」という苦情が殺到
  →POP before SMTPを導入することにより、とりあえずは解決。

SPAMメール対策(2)

- POP before SMTPとは？
  まず、POP接続をしてユーザーとパスワードを確認し、問題がなければ、そのIPアドレスからのSMTP通信を一定時間開放する手段。
- Outlook Expressでは、いまだに送信→受信という流れのため、OEユーザーにはちょっと使いにくい。

SPAMメール対策(3)

- (1)に対する対策
  携帯会社・無料メール会社による大量投稿制限により、現在ではかなり減少
- (2)に対する対策
  クライアントマシンがISPのサーバーを通さず、直接MXレコードを引き送信するようになり、対策が困難。ISPが各ユーザーに対して警告するなどして対策。ただし、差出人の詐称なども行われており、非常に特定は難しい。

なぜ難しいか？

- SMTPという仕組み自体が、MUAとメールサーバーとの通信手段であるのと同時に、メールサーバー同士の通信手段であるため、制限をかけにくい。

では、どうすれば良いか？

- MUAから、無関係のISPへのメールを、遮断してしまえば良いじゃないか！
  →outbound port 25 Blockingの考えの基本

Outbound port 25 Blockingの弊害

- 単純に外部へのSMTP接続をフィルタしてしまうと、外部ISPのメールサーバーを使った送信が使えなくなってしまう。
  →再び外部ISPのメールサーバーが使えなくなり、ユーザーから不満の声が上がる。
- 対策: MTAがメールを送信するためのポートと、MUAからメールを受け付けるためのポートを分け、後者は認証をする(submission port+SMTP AUTH)

参考資料: Outbound port 25 Blocking(OP25B)を導入している大手プロバイダ(導入予定・一部導入等も含む)

- NTT系(OCN, wakwak,ぷらら、InfoSphere)
- IIJ系(IIJ4u,IIJmio)
- その他(@Nifty, DION, BIGLOBE, sannet, TikiTiki等)

自宅サーバーを立ち上げている場合は、どうするべきか？

- OP25Bを導入していないプロバイダに乗り換える(エックス・チェンジでは現在何も制限していないので、何でもあり)
  →将来的に制限の可能性もあり
- 固定IPを取得している場合、OP25Bの制限から外れている場合もあるので、プロバイダのサポートページ等を確認し、固定IPを取得する
- 今回は、自宅サーバーにsubmission portをサポートしたメールサーバーを立てることを目標とする。

目標その1:
POP defore SMTPの設定(1)

- ターゲットマシンの環境: FreeBSD 6.0-RELEASE-p1+2006/01/01現在のports
- IPv4/IPv6のリーチャビリティは一応ある。

POP before SMTPの設定(2)

- とりあえず、POP before SMTPは基本でしょう。と言う事で、DRAC(Dynamic Relay Authorization Control)を用いて認証する設定を入れてみる。
- /usr/ports/mail/dracをコンパイル。
- /usr/ports/mail/qpopperを、WITH_DRAC=yes でコンパイルする。

POP before SMTPの設定(3)

- /etc/rc.conflに、次の設定を入れる。
  dracd_enable="YES"
  dracd_flags="-i -e 15"
  rpcbind_enable="YES"
- /usr/local/etc/dracd.allow.sampleを/usr/local/etc/dracd.allow にコピーし、上の行をコメントアウト(localhostのみ使用)

POP before SMTPの設定(3)

- /etc/mail/FQDN.mc に、以下の行を追加

```
LOCAL_CONFIG
Kdrac btree /usr/local/etc/dracd LOCAL_RULESETS
SLocal_check_rcpt
R$*             $: $&{client_addr}
R$+             $: $(drac $1 $: ? $)
R?              $@ ?
R$+             $@ $#OK
```

- POPで認証すると、15分間はそのIPアドレスからメールが送信できる。
- portmapを使うので、enableにする。

目標その2: SMTP AUTHの設定(1)

- /usr/ports/mail/sendmail-sasl をmake, make install する。(OSの標準機能としてSASL付きsendmailの作成はサポートしているが、ここでは使わない)
- SASL(Simple Authentication and Security Layer): RFC2222
  汎用的な認証の枠組みを提供
  認証手段: CRAM-MD5(RFC2195), DIGEST-MD5(RFC2831), PLAIN(RFC2595), LOGIN

SMTP AUTHの設定(2)

- Outlook ExpressはPLAINのみサポートなので、サポートが必要であろう。(ただし、所詮は生パスワードなので、後述するSTARTTLSも加えて、暗号化するほうがbetter)
- Becky! などは、CRAM-MD5, LOGIN, PLAINなどをサポートしているので、とりあえず全部サポートとする。

SMTP AUTHの設定(3)

- make installすると、sendmailが/usr/local/sbinにインストールされるので、インストールしたあと、/etc/mail/mailer.confを書き換え、そちらのsendmailが起動するようにする。
- # **cat /usr/local/lib/sasl2/Sendmail.conf**
  pwcheck_method: saslauthd
  となっていることを確認し、/etc/rc.confに、**saslauthd_enable="YES"** を追加。
- /usr/local/etc/rc.d/saslauthd.sh start を実行。

SMTP AUTHの設定(4)

- /etc/mail/FQDN.mcの編集

```
dnl set SASL options
TRUST_AUTH_MECH(`CRAM-MD5 DIGEST-MD5 LOGIN PLAIN')

define(`confAUTH_MECHANISMS', `CRAM-MD5 DIGEST-MD5 LOGINPLAIN')
```

- /etc/mailでmake, make installし、sendmailをリスタートする
- これで一応、SMTP AUTHがサポートされたsendmailが起動するはず。

SMTP AUTHの動作チェック

- telnet サーバー名 25とかした後、EHLO localhostとか入力したときに、
  250-AUTH LOGIN PLAIN DIGEST-MD5 CRAM-MD5
  と返事が返ってくればOK
- クライアントの動作をチェックする場合、OEだったら、「このサーバーは認証が必要」にチェックを入れて、メールが送信できればOK

SMTP AUTHをsubmission portで動かす(1)

- このままでは、SMTP AUTHによる認証はできるが、OP25Bの問題は解決できていないので、submission portを有効にする。
- /etc/mail/FQDN.mcを次のように変更

```
FEATURE(`no_default_msa')
DAEMON_OPTIONS(`Name=MTA-v4, M=C, Family=inet')
DAEMON_OPTIONS(`Name=MTA-v6, M=C, Family=inet6')
DAEMON_OPTIONS(`Port=587, Name=MSA-v4, M=Ea,
Family=inet')
DAEMON_OPTIONS(`Port=587, Name=MSA-v6, M=Ea,
Family=inet6')
```

SMTP AUTHをsubmission portで動かす(2)

- パラメータの意味合い
  ごく大雑把に説明すると、port 587番で
  SMTP AUTH付きでメールを受信するよう
  に設定

SMTP AUTHの弊害・対策

- OEからのSMTP AUTHは、生パスワードを流す認証のため、パスワードの盗聴等の可能性がある。そのため、TLS(Transport Layer Security): RFC2246を併用して通信路の暗号化をした方がよい。今回は、STARTTLS(SMTP service Extention for Secure SMTP over TLS)を導入する。

TLS化の方法(簡略化バージョン)(1)

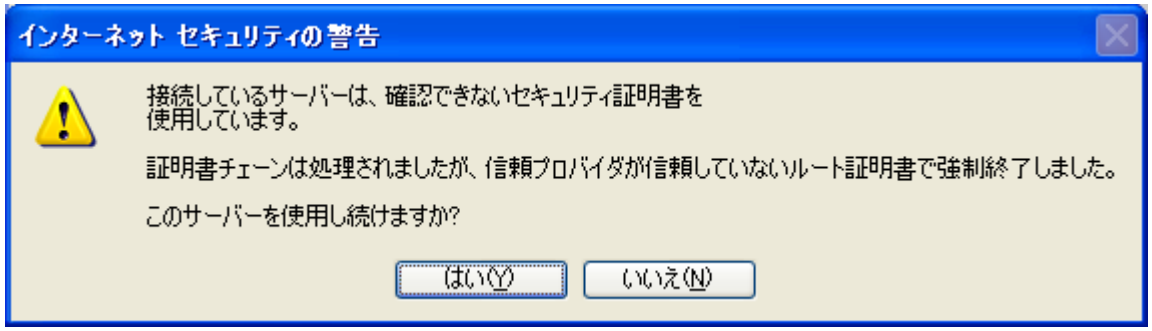
- # cd /etc/mail
  # mkdir certs
  # chmod 700 certs
  # cd certs
  # openssl req -new -x509 -nodes -out cert.pem
  (opensslのメッセージは略)
  # chmod 600 *.pem
  # cd ..
  /etc/mail/FQDN.mcを編集
  # make cf install
  # /etc/rc.d/sendmail restart

TLS化の方法(簡略化バージョン)(2)

- /etc/mail/FQDN.mcは、以下を追加する
  define(`confCACERT_PATH', `/etc/mail/certs')dnl
  define(`confCACERT', `confCACERT_PATH/cert.pem')dnl
  define(`confSERVER_CERT', `confCACERT_PATH/cert.pem')dnl
  define(`confSERVER_KEY', `confCACERT_PATH/privkey.pem')dnl
- telnet サーバー名 25とかした後、EHLO localhost とか入力したときに、
  250-STARTTLS
  と返事が返ってくればOK

OEの設定変更

- 詳細設定のタブで、「このサーバーはセキュリティで保護された接続(SSL)が必要」にチェックを入れて、メール送信をする。



- おれおれ証明書(^^;のため、以下のメッセージが出るが、無視して進める。(実運用では証明書を取ってください)

STARTTLSの現在未解決な問題

- STARTTLSを有効にすると、SMTP portが強制的に25になってしまう。無理やりport 587に書き換えてみたが、メールは送信できなかった。
  →STARTTLSを使うと、OP25Bに対応できない？
- STARTTLSを使ったISPは今のところ少ない
- SMTP over ssh とかで逃げる？

目標その3: make buildworldでSMTPAUTH対応sendmailを作る

- 下準備
  (1) portsで、cyrus-saslとcyrus-sasl-saslauthdが入っていることを確認(入っていなければ入れる)
  (2) /etc/make.conf で、
  SENDMAIL_CFLAGS=-I/usr/local/include -DSASL=2
  SENDMAIL_LDFLAGS=-L/usr/local/lib
  SENDMAIL_LDADD=-lsasl2
  を定義して、make buildworld, make installworld する
  (3) /etc/mail/FQDN.mc をそれなりに直して、make installする

まとめ

- SMTP AUTHとsubmission portを利用することで、OP25B対策を取っているプロバイダからでも、他のプロバイダを利用してメール送信をすることが可能になる。
- これからの動向として、OP25Bが主流となりつつあると考えられるので、submission port+SMTP AUTHを導入したsendmailを自宅・会社のサーバーにすることをお勧めします。

参考資料(1)

- http://www.debug.gr.jp/events/20010414/presentation/smtpauth/index.html
- http://www.imasy.or.jp/~ume/presentation/CBUG-20041002/
- http://www.fkimura.com/sendmail-cf1.html
- http://www.fkimura.com/sendmail-cf15.html
- http://www.fkimura.com/drac0.html
- 各社プロバイダのWebサイト

参考資料(2)

- Impress internet watch
- http://www.jeag.jp/ (Japan E-mail Anti-abuse Group)
- https://www.iijmio.jp/guide/outline/mm/#security
- http://www.wakwak.com/info/spec/port25/
- http://www.plala.or.jp/access/living/releases/nr05_aug/0050830.html