Submissionポートの提供
方法と実践

iprio
.com

パナソニック ネットワークサービシズ株式会社
テクニカルプロデュースグループ
池田武　ikeda@pana.net

株式会社イプリオ
代表取締役
石田卓也 takuya@iprio.co.jp

あるメールサーバの実情

- 自ドメイン宛：中継＝８：１
- 自ドメイン宛のうち送信者偽装が９０％
  - OP25Bの普及により国内は減少傾向
  - 海外からのメールが増加傾向（BotNet?）
- 中継のうち送信者偽装が７０％
  - ISPネットワーク内からPort２５を使用しての送信が増加傾向。
  - 数年前は中継での送信者偽装はほとんどなかった。
  - Submission（SMTP-Auth）の普及が急務
- 中継メール上位宛先ドメイン
  - aol.com　３５％　From:はランダム
  - comcast.net　３５％　From:はランダム
  - yahoo.co.jp　４％　From:は半数ランダム、半数が自ドメイン
- SMTP-Auth利用率
  - 全メール利用者の0.5％

あるプロバイダの実情

- 長期休暇前にサーバのレートコントロールを厳しくした。
  - 休暇中は手動対応が遅くなるための一時的対応 (緊急避難)
  - 同一のIPから１０分間当たり1000通。
  - 一般的な端末からのメール送信であればありえない数。
- 休暇中にCSにクレームがあり緊急対応。
  - Yahoo!オークションや日経BPなどからのメールについては個別にホワイトリストで対応していた。
  - リストからもれていた大規模メールマガジンからのメールを誤って拒否。
- MTAとMSAが分離されていないため発生した事故。

Submissionの実現方法

- Sendmail,Postfixを１つで実施する方法。
  - 簡単に実現可能。
- Sendmail,Postfixを２つで実施する方法。
  - 設定は複雑。
  - 細かいレートコントロールやフィルタの適用が可能。
- 他のMTA製品を使用している場合。
  - 本来はMTA製品で対応するほうが、運用面・性能面でよいと思われる。
  - MSAとしてのみsendmail,postfixを使用することで、暫定的に対応可能。
  - バージョンアップ等に時間がかかる場合など。

Submission実装の考え方

- SMTP Auth を使用する(必須)。
  - SASLを利用する形でコンパイルするMTAがほとんど。
- MTAとMSAを分離する（必須）。
  - 可能ならばポートだけではなくIPアドレスも別のものにするのがよい。
- POP before SMTP はやめる。
  - 認証したアカウントを知ることが困難。NATの問題も。
    - アカウントごとのアクセス制限が行いづらい。
    - ログからspammerを発見するのにRADIUSの接続ログと突合せが必要。
- TLSを使用可能にする（必要に応じて）。
  - 通信経路暗号化によるセキュリティの強化。
  - クライアントサポート、証明書取得の問題あり。
  - これから対応するなら、SMTP over SSL は使用しないほうが良い。
    - SMTP over SSL のポート465は、公式には別用途に割り当てられている。
    - すでに SMTP over SSL を実装しているのであれば、あえて止める必要はない。

SASLとは

- Simple Authentication and Security Layer
- アプリケーションに依存せずに認証のメカニズムを実現する
  - Sendmail+SASL、Postfix+SASLなど
- 最新のOSには入っていることが多い
  - Sendmailの場合、sendmail –d0.10 でCompiled with: に SASL が入っていれば使用可能。入っていない場合はコンパイルでSASLを指定。
- /usr/lib/sasl2 または /usr/local/lib/sasl2 の下に設定などを置く
  - バージョン1の場合は、/usr/lib/sasl 配下
  - Sendmail.conf または smtpd.conf中で以下の設定をする。
  - pwcheck_method:ｘｘｘｘ … 認証に使用するプログラムを指定
    - saslauthd … /etc/shadow, PAM, LDAPなどの認証メカニズムに対応。/etc/shadowやPAMを使用する場合は、PLAIN/LOGINのみ。
    - pwcheck … /etc/shadow を使用。PLAIN/LOGINのみ
    - sasldb (v1) … sasl自身のデータベースを使用。MD5使用可。
    - auxproc (v2) … sasl自身のデータベースを使用。MD5使用可。

LinuxでSASLを使用する場合

- /etc/rc.d/init.d/saslauthd が既にあるので有効化する。

```
# chkconfig --list saslauthd
saslauthd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
# chkconfig saslauthd on
# chkconfig --list saslauthd
saslauthd       0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

- /usr/lib/saslの下に設定ファイルがあるので変更する。
  - Sendmail.conf(Sendmailの場合),smtpd.cong(postfixの場合)

```
pwcheck_method: saslauthd
```

- これで、/etc/shadowによるAuthの準備が完了。
- 他のソースで認証させたい場合は、/etc/sysconfig/saslauthd内で設定を書けば反映される。
  - 例：MECH=pam　MECH=ldap

他のOSの場合

- Solaris
  - Cyrus-SASLの公式サイト(カーネギーメロン大学)から入手してコンパイル
    ftp://ftp.andrew.cmu.edu/pub/cyrus-mail/
  - sunfreewareからPackageも手に入る
    http://www.sunfreeware.com/
  - Solaris10に付属のSASLはライブラリが足りない
- FreeBSD
  - Ports,Packageなどから入手
  - もちろんsourceからでも

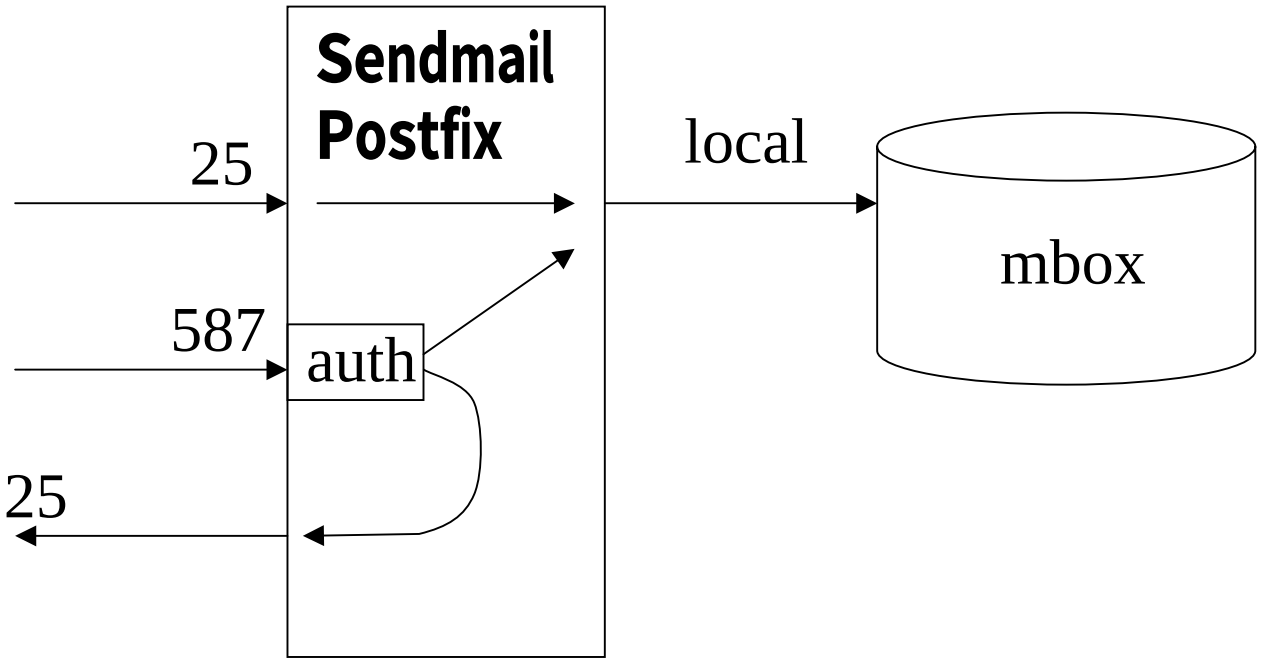
CRAM-MD5・DIGEST-MD5を使用するか？

- PLAIN/LOGIN
  - 暗号化されていない生パスワードが流れる（単にエンコード）
  - /etc/shadow などが使用できるので、生パスワードを持たなくてよい
  - POP、radiusなど現状パスワードの利用が容易
  - ISPのお客様の9割が使用している OutlookExpressは、LOGINのみ。

- CRAM-MD5/DIGEST-MD5
  - チャレンジ＆レスポンス方式により、生パスワードが流れない
  - サーバに生パスワードを持つ必要がある
  - POPとのパスワード共用には何らかの工夫が必要(APOPなど)

→ ISPで使用するのであれば、PLAIN/LOGINで充分ではないか
  - 必要ならSSLやTLSを使用して経路自身を暗号化すればよい

Submission実装　その1（同一デーモン）



※Postfixは複数のデーモンで処理する

Sendmailでの設定例

- Sendmailは、8.12より標準でSubmissionに対応している。
  - 単純にSubmissionに対応するだけではだめ。
  - SMTP Authを必須とする必要がある。
  - SASLオプションをつけてBuild。
- O'REILLY Sendmail 3rd Edition の§10.9を参照して、サーバの環境に合わせたauthの基本設定を行う。
- ファイル内に、次の記述をする。
  - §4.8.30、§24.9.24 を参照。
  - §10.9.3の最終行の設定 (F=a)は間違い！

```
FEATURE(`no_default_msa')
FEATURE(`authinfo')
FEATURE(`virtusertable')
FEATURE(`access_db')
define(`confAUTH_MECHANISMS',`CRAM-MD5 LOGIN PLAIN')
define(`confDOMAIN_NAME',`mail.example.com')
TRUST_AUTH_MECH(`LOGIN PLAIN')
DAEMON_OPTIONS(``Port=25,Name=MTA'')
DAEMON_OPTIONS(``,Port=587,Name=MSA,M=Ea'')
```

※認証にLDAP等を使っている場合は、適切な設定に書き換える

Postfixでの設定例

- Postfixも、現在では標準でSubmissionに対応している。
  - ただし、設定ファイルでコメントアウトされているので有効に。
  - SMTP Authを必須とするのも忘れずに！
  - SASLオプションをつけてBuild。

```
make makefiles CCARGS='-DUSE_SASL_AUTH –I/usr/local/include/sasl' AUXLIBS='-L/usr/local/lib –lsasl2'
※ -rpath /usr/local/lib や-R/usr/local/libが必要なOSも
```

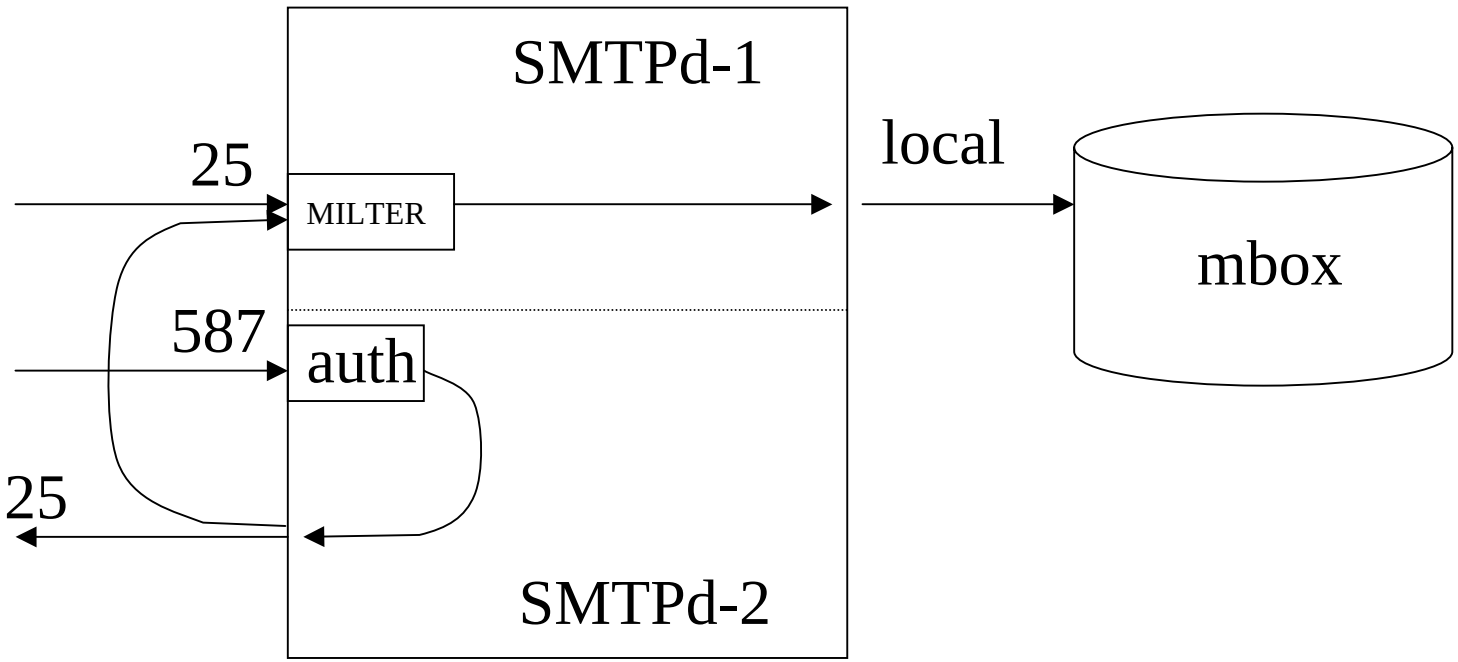
- サーバの環境に合わせたauthの基本設定を行う。

```
/usr/local/lib/sasl2/smtpd.conf に pwcheck_method: saslauthd など
main.cf に smtpd_sasl_auth_enable = yes
```

- Submitポートを有効に。

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
submission inet n      -       n       -       -       smtpd
       -o smtpd_etrn_restrictions=reject
       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

Submission実装　その2(2つのデーモン)



sendmail.cfを2個にする理由

- MTAとして外部のメールサーバから受信するポートと、MSAとしてユーザの端末から受信するポートでは異なったレーティングを行うことが望ましい。
- rate-control 、spam-filter、virus-filter 等で使用する MILTERは、一つのsendmail.cf内では受信ポートごとの設定ができない。
- 設定を2つ持つことにより将来、規模の拡大等でMTAとMSAを物理的に分離する必要がでたときに拡張が容易になる。
- DNSBLなどの利用も簡単に実装できる。
- 応用で、Sendmail + Postfix といった複数のMTAを使うことも可能。

Sendmailで、cfを2個にする設定例

- 一台のサーバに複数のIPを設定する。
- mcファイル1（MTA用）。

```
FEATURE(`no_default_msa')
FEATURE(`virtusertable')
FEATURE(`access_db')
define(`confDOMAIN_NAME',`mta.example.com')
define(`QUEUE_DIR',`/var/spool/mqueue.mta')
definr(`confPID_FILE',`/var/run/sendmail.mta.pid')
DAEMON_OPTIONS(``Addr=192.168.1.1,Port=25,Name=MTA")
```

- mcファイル2（MSA用）。

```
FEATURE(`no_default_msa')
FEATURE(`authinfo')
define(`confAUTH_MECHANISMS',`CRAM-MD5 LOGIN PLAIN')
define(`confDOMAIN_NAME',`mail.example.com')
define(`QUEUE_DIR',`/var/spool/mqueue.msa')
definr(`confPID_FILE',`/var/run/sendmail.msa.pid')
TRUST_AUTH_MECH(`LOGIN PLAIN')
DAEMON_OPTIONS(``Addr=192.168.1.2,Port=25,Name=MSA25,M=Eab")
DAEMON_OPTIONS(``Addr=192.168.1.2,Port=587,Name=MSA,M=Eab")
※このcfでは、他からのアクセスはすべて拒否するため、access_dbを使用しない
※認証にLDAP等を使っている場合は、適切な設定に書き換える
```

- DNSの設定。

```
@       MX      mta.example.com
mta     IN A   192.168.1.1
mail    IN A   192.168.1.2      ※利用者のメールソフトの設定が、mail.example.com　の場合
```

Postfixを２つ稼働させる設定例

- 一台のサーバに複数のIPを設定する（ifconfig等）
- 元の設定ファイルを、別ポート用のディレクトリに移動

```
# cp -rp /etc/postfix /etc/postfix-msa
```

- 新しいmain.cfを変更

```
queue_directory = /var/spool/postfix-msa
alternate_config_directories = /etc/postfix-msa
inet_interfaces = mta.example.com
smtp_bind_address = 192.168.1.2
```

- 新しいmaster.cfも変更（前ページのSendmailと同じ設定）

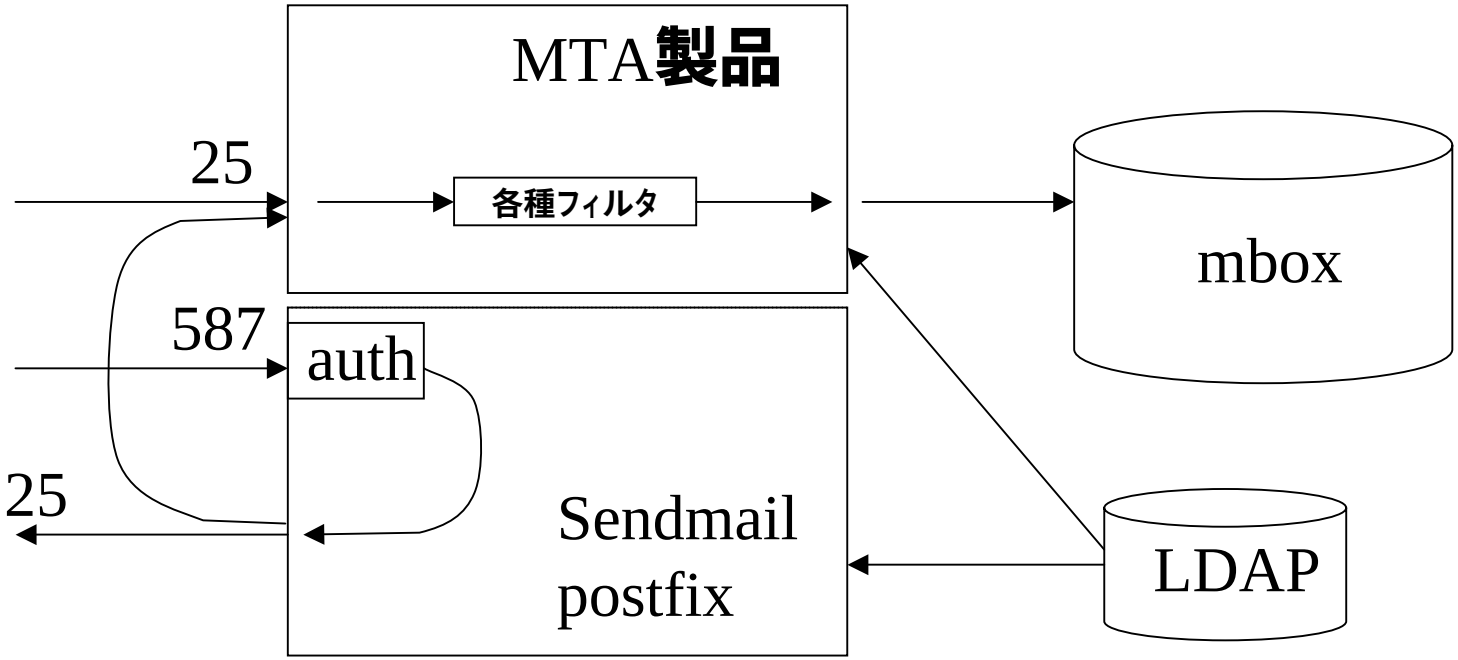
```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
       -o smtpd_client_restrictions=permit_sasl_authenticated,reject

submission inet n      -       n       -       -       smtpd
       -o smtpd_etrn_restrictions=reject
       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

- 起動スクリプトの設置など

```
# postfix -c /etc/postfix-msa start
```

MTA製品との組み合わせ



- MTAによっては、SMTPauth必須に対応していない場合がある。
- MTA製品で対応可能になるまでの中継ぎに sendmail を使用。
- 現状ではMSAのトラフィックはMTAの1/10以下なので、最小限の投資で実現可能。

今回説明した以外のMTA

(参考)
・現在の大体の最新版

MTA	Submission	SMTP-Auth
qmail	RELAYCLIENTなし、rcpthosts を有効にしたものをtcpserverやxinetdで587で作動させる	smtp-auth-patch など
exim (v4)	daemon_smtp_ports = 25 : 587 acl_check_mail:	saslなど
courier	/usr/lib/courier/etc/esmtpd-msa に別ファイルを設定し、makesmtpaccess-msa	独自対応(authlib)

ケーススタディ～地方ISPの場合

- 引き金は、大手ISPのOP25Bの実施
  →顧客から、「メールが送れない」という苦情が
- Submissionポートの提供はすぐに決定
  →Sendmailで、すでに空いていた
- POP before SMTPの廃止を決定
- Submissionポートの認証(SMTP AUTH)必須化、公開
- 当初、PLAINのみで提供
  →Outlook Expressのユーザが使えない
  →LOGINにも対応
- TLSにも対応を予定