

smf-spf で SPF

幸せの便りは届くか!?

Echigo BSD Users Group 23th meeting
at Nagaoka city Citizen Center.
15th, September, 2007
INOUE Mikio <mikio@ebug.jp>

おしながき

- smf-spf の紹介
- インストールの実際
- 動作確認

smf-spf

- Smart Sendmail filters
 - 軽くて早い Sendmail filter がいろいろ。
 - 機能の拡張もいろいろ。
 - 安心して使っているのかは不明。
 - <http://smfs.sourceforge.net/smf-spf.html>
- smf-spf
 - 最新版は v2.0.2 (Jan 10 2007)

smf-spf v2.0.2 の特徴

- いろんな Whitelist が使える
 - IP, PTR, Envelope Sender, Envelope recipient
- In-memory cache engine
- SMTP AUTH 対応
- SPF Fail/SoftFail の場合の処理がいろいろ
 - 隔離モード、Subject: のタギング他
- その他

導入に必要なもの

- FreeBSD/Linux/Solaris
- Sendmail v8.11 以降
 - MILTER API を有効にして make したもの
- BIND8
 - メールサーバ上で動いていることが望ましい。
- libSPF2 v1.2.5 以降
 - ports から入れました。

Makefile の編集

- Tarball に入ってるのは Linux 用
 - FreeBSD 用エントリも書いてあるので、コメントを処理するだけ。
 - Sendmail v8.11 用のエントリもあるけど、今回導入した Sendmail v8.13 ではおかしくなったので、コメントアウトしたままにしました。

コンパイルとインストール

- su で make; make install だけ
 - 数秒で終わります。
 - smfs というユーザとグループを勝手に作ります。
- Tarball の init/ に各 OS 用の起動スクリプトが用意されてます。
 - 適当に名前を変えて /usr/local/etc/rc.d に入れておきましょう。

smf-spf のテスト

- 設定は、とりあえずデフォルトのまま
- 起動スクリプトから実行する
 - /usr/local/etc/rc.d/smfspf start
 - smf-spf が実行ユーザ smfs で動いてるか確認する。
 - ソケット /var/run/smfs/smf-spf.sock ができてるか確認する。

設定ファイルの編集

- /etc/mail/smfs/smf-spf.conf
 - 自 IP アドレスを IP WhiteList に追加。
 - 認証に失敗したメールの処理を変更。
 - RefuseFail off。
 - 大事なまで消えると怖いので、当面様子を見るためです。
 - 設定ファイルは起動時に読み込むので、変更したら smf-spf を再起動すること。

mc ファイルの編集

- 2 行追加するだけ
 - smf-zombie, smf-sav, smf-grey などを使ってる場合は、順序が指定されるので注意。
- ```
define('confMILTER_MACROS_HELO', confMILTER_MACROS_HELO, '{verify}')dnl
INPUT_MAIL_FILTER('smf-spf', `S=unix:/var/run/smfs/smf-spf.sock, T=S:30s;R:1m`)dnl
```
- make して sendmail.cf を作る。
  - make restart で Sendmail を再起動。

## 動作確認 1/2

- ログは /var/log/maillog に出ます。
  - 設定ファイルで syslog のファシリティを変更できます。
- メールが流れてるか確認します。
  - ヤバければ、sendmail.cf を戻して、Sendmail を再起動してください。

## 動作確認 2/2

- こんな感じのログが残ります。

```
SPF pass: xxx.xxx.xxx.xxx, spf.example.jp, spf.example.jp, mikio@example.jp
SPF none: xxx.xxx.xxx.xxx, nospf.example.jp, nospf.example.jp, mail@nospf.example.jp
SPF softfail: xxx.xxx.xxx.xxx, [xxx.xxx.xxx.xxx], spf.example.jp, mail@uso.example.jp
SPF fail: xxx.xxx.xxx.xxx, nospf.example.jp, nospf.example.jp, mail@example.jp
```
- 受け取ったメールにもヘッダが付加されます。

```
Received-SPF: Pass (ns.example.jp: domain of mail@spf.example.jp designates
xxx.xxx.xxx.xxx as permitted sender) receiver=ns.example.jp; client-
ip=xxx.xxx.xxx.xxx; envelope-from=<mail@spf.example.jp>; helo=spf.example.jp;
```