Clam AV の紹介

知らんヤツっているのか!?

Echigo BSD Users Group 25th meeting
at Nagaoka city Civic Center 204.
16th, February, 2008
INOUE Mikio <mikio@ebug.jp>

おしながき

- ClamAV の紹介
- 導入
- 運用
- 感想

- 参考
  - Clam AntiVirus http://www.clamav.net/

Clam AntiVirus

- ウィルス対策ツールキット
  - オープンソース (GPL)。
  - コマンドラインスキャナ / オンアクセススキャナ
  - Sendmail 用 milter インターフェイス。
  - 機能の拡張もいろいろ。
  - エンジン部分はシェアードライブラリ。
  - 各種メール形式や文書形式、圧縮ファイルにも対応。

インストール 1/2

- FreeBSD の ports からだと一発コンパイル。
  - 実行ユーザ clamav:clamav が作成されます。
- /usr/local/etc/freshclam.conf の変更。
  - ウィルス DB の指定。(必須)
    - db.jp.clamav.net
  - 更新頻度の指定。
    - デフォルトは、毎日 12 回 (起動時から 2 時間毎)。

インストール 2/2

- ClamAV の milter を有効にする。
  - /etc/mail/sendmail.mc に次の 2 行を追加して make。

```
INPUT_MAIL_FILTER(`clmilter', `S=local:/var/run/clamav/clmilter.sock, F=,
    T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clmilter')dnl
```

- ブート時の自動起動の設定。
  - /etc/rc.conf に次の各行を追加。

```
clamav_clamd_enable="YES"
clamav_clamd_flags=""
clamav_clamd_socket="/var/run/clamav/clamd"
clamav_milter_enable="YES"
clamav_milter_socket="/var/run/clamav/clmilter.sock"
clamav_milter_flags="--postmaster-only --local --outgoing --timeout=0 --max-
    children=50"
clamav_freshclam_enable="YES"
```

デーモン

- clamd
  - Clamav の本体
  - コマンドとしても使えます。
- freshclam
  - データベース自動更新用デーモン
- clamav-milter
  - メールスキャナデーモン

コマンド

- clamscan
  - コマンドラインスキャナ
- clamconf
  - 設定ユーティリティ (使ったことない)
- sigtool
  - データベース管理ツール (使ったことない)

動作確認 1/2

- /var/log/clamav/freshclam.log (重要)

```
freshclam daemon 0.92 (OS: freebsd6.3, ARCH: i386, CPU: i386)
ClamAV update process started at Mon Feb 11 23:38:19 2008
main.inc is up to date (version: 45, sigs: 169676, f-level: 21,
   builder: sven)
Downloading daily-5772.cdiff [100%]
Downloading daily-5773.cdiff [100%]
Downloading daily-5774.cdiff [100%]
daily.inc updated (version: 5774, sigs: 39241, f-level: 21, builder:
   ccordes)
Database updated (208917 signatures) from db.jp.clamav.net (IP:
   61.205.61.201)
Clamd successfully notified about the update.
```

- /var/log/clamav/clamd.log

動作確認 2/2

- メールヘッダの追加などを確認。
  - 自分宛にメールを出してテストすると、次のようなヘッダがついてます。

```
X-Virus-Scanned: ClamAV 0.92/5781/Tue Feb 12 16:50:56 2008 on ns.pagans.jp
X-Virus-Status: Clean
```

運用

- バージョンアップが多いので注意。
  - セキュリティホールは少ないけど、通常 1〜3 ヶ月毎に新しいのが出ます。
  - 古いのを使ってると /var/log/clamav/freshclam.log に警告がでます。

```
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.90.1 Recommended version: 0.90.2
DON'T PANIC! Read http://www.clamav.net/support/faq
```

  - ウィルス DB の情報を活用できなくなる場合が多いので注意。

感想 1/2

- いくつかのサイトで、クライアントに入ってる市販のウィルススキャナによって検出された、メールに添付されたウィルスは全くありません。
- 出て行くメールも検査してくれます。
- クライアント管理が難しいサイトでは、大きな効果が期待できます。

感想 2/2

- ウィルス名が各社のものと全く異なる。
  - 特定のウィルスが世間で騒がれても、区別がつきません。
- Phishing メールも排除します。
  - 但し、ウィルスと処理を区別できません。
- バージョンアップを自動化して欲しい。