はじめに

Tripwire みたいな、ファイルの改竄を検出するなにか、のめも。

最近では、ホストベース IDS とかいうみたい。ものは言いようだねー。

おしながき

mtree

BSD 系 UN*X には昔からついているコマンド。(OS X にも入っている。)NetBSD 3.0 の man には、

```
HISTORY
     The mtree utility appeared in 4.3BSD-Reno.  The optional keyword appeared
     in NetBSD 1.2.  The -U flag appeared in NetBSD 1.3.  The flags and md5
     keywords, and -i and -m flags appeared in NetBSD 1.4.  The device,
     rmd160, sha1, tags, and all keywords, -D, -E, -I, -l, -L, -N, -P, -R, -W,
     and -X flags, and support for full paths appeared in NetBSD 1.6.  The
     sha256, sha384, and sha512 keywords appeared in NetBSD 3.0.
```

ってのっている。

- man: FreeBSD 6.2・NetBSD 3.0(NetBSD 本家 = man.netbsd.org はどうもデータが壊れているので、FreeBSD 本家のリンク)・OpenBSD 4.1。
- 『BSD HACKS』には Tripwire みたいな使い方の解説 (Hack #58) がのっている。
- NetBSD では、/etc/mtree/DIR 名 .secure という名前で、改竄検知用のデータを作っておけば、/etc/security.conf の check_mtree を yes にすると、検知対象とすることができる。/etc/security のコメント部を読んでみよう。
- google ればいろいろでてくるよ。http://www.bsdforums.org/forums/archive/index.php/t-4257.html とか。
- Linux や他の OS でも使いたい
  - Linux への移植版 mtree。でも最近の Linux だと、make とおらないみたい。
  - Openwall GNU/*/Linux にも、FreeBSD から移植された mtree がある。
    - 上記のを、Vine 2.5 で使えるように SRPM() にしてみた。無保証だよ。
  - debian にも deb が freebsd-mtree とかってあったような気が？でも探してもないんだよね。
  - pkgsrc の bootstrap kit(ftp) にも、mtree がある。これだと、Solaris とかでも make さえとおれば使える。
  - gentoo には portage がある。上記 bootsrtap kit の mtree みたい。

AIDE

http://aide.sourceforge.net/

NetBSD の人は "Installing and configuring AIDE for NetBSD" を見よう。

orisis

http://www.hostintegrity.com/osiris/

samhain

いきなり Javascript。w3m ではなにも見えない。;_; 見えるようになった。

http://samhain.sourceforge.net/

integrit

http://sourceforge.net/projects/integrit/

更新は止まっているっぽい。

find **とかでがんばる**

```
find /path/to/dir -ls > file1
find /path/to/dir -type f | xargs sha1sum >> file2
```

とかでがんばるとか。