Panda TruPrevent を使ってみました
～あるいは仮想インターネットの実装～

小島肇　kjm@rins.ryukoku.ac.jp
龍谷大学理工学部

前回までのあらすじ

ふるまい検出?

- Cisco Security Agent
- Panda TruPrevent
- ホストベース IPS
- どのくらい使えるものなのか要検証

Panda TruPrevent

Panda TruPrevent

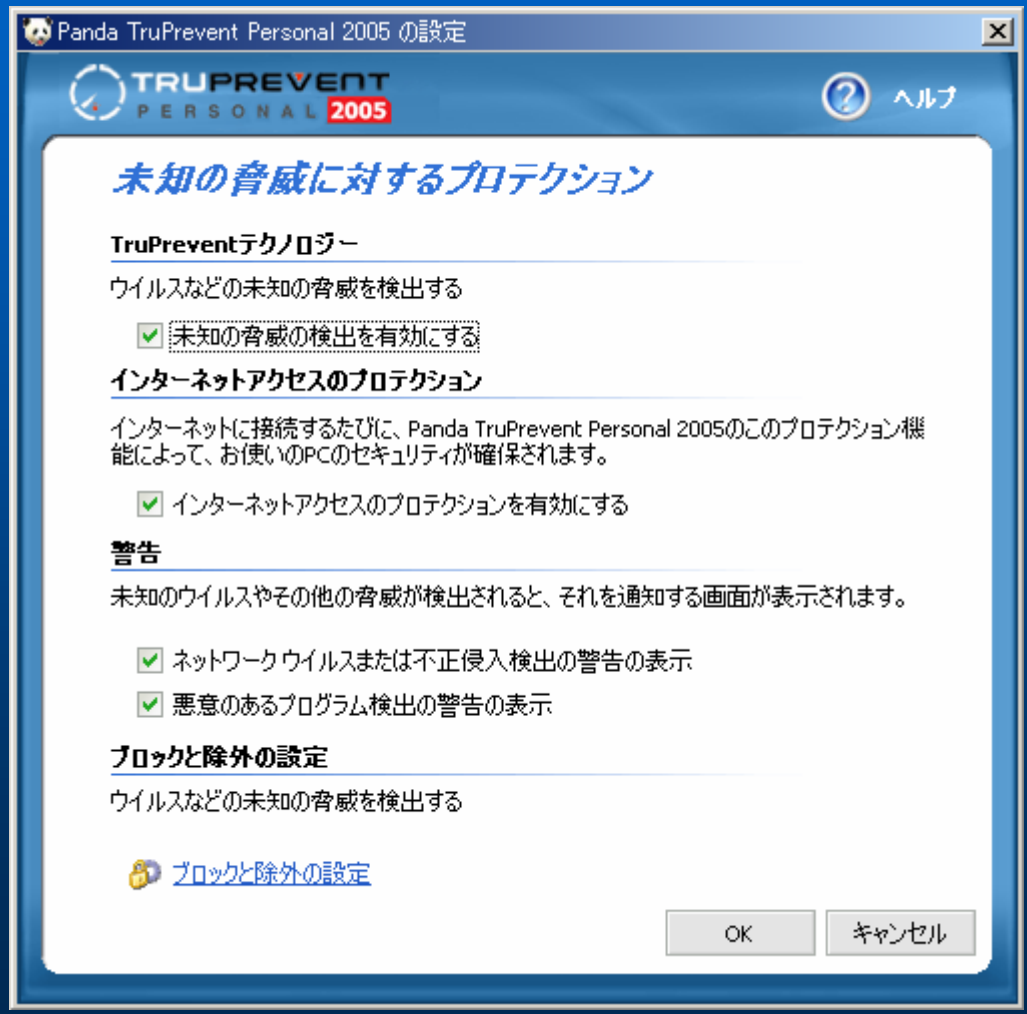
- Panda Software（本社:スペイン）の製品
  http://www.pandasoftware.jp/
  - www.Panda.co.jp から引用:
    TruPrevent Personal 2005は、他のアンチウイルス製品では不可能な処理を実行します。つまり、アンチウイルスでは阻止しきれなかったプログラムの振る舞いを分析して未知のウイルスを検出、瞬時にその動作をブロックします。
- Personal 版と Corporate 版がある
  - Personal 版はほとんどチューニングできない（おまかせ）
  - Corporate 版はある程度のチューニングが可能（設定項目はそれほど多くはなさそう）

TruPrevent Personal 試用版を get

- 情報セキュリティ Expo（6/29～7/1）: Panda ブース
- インストーラ→
- インストール自体はごくふつうに終了

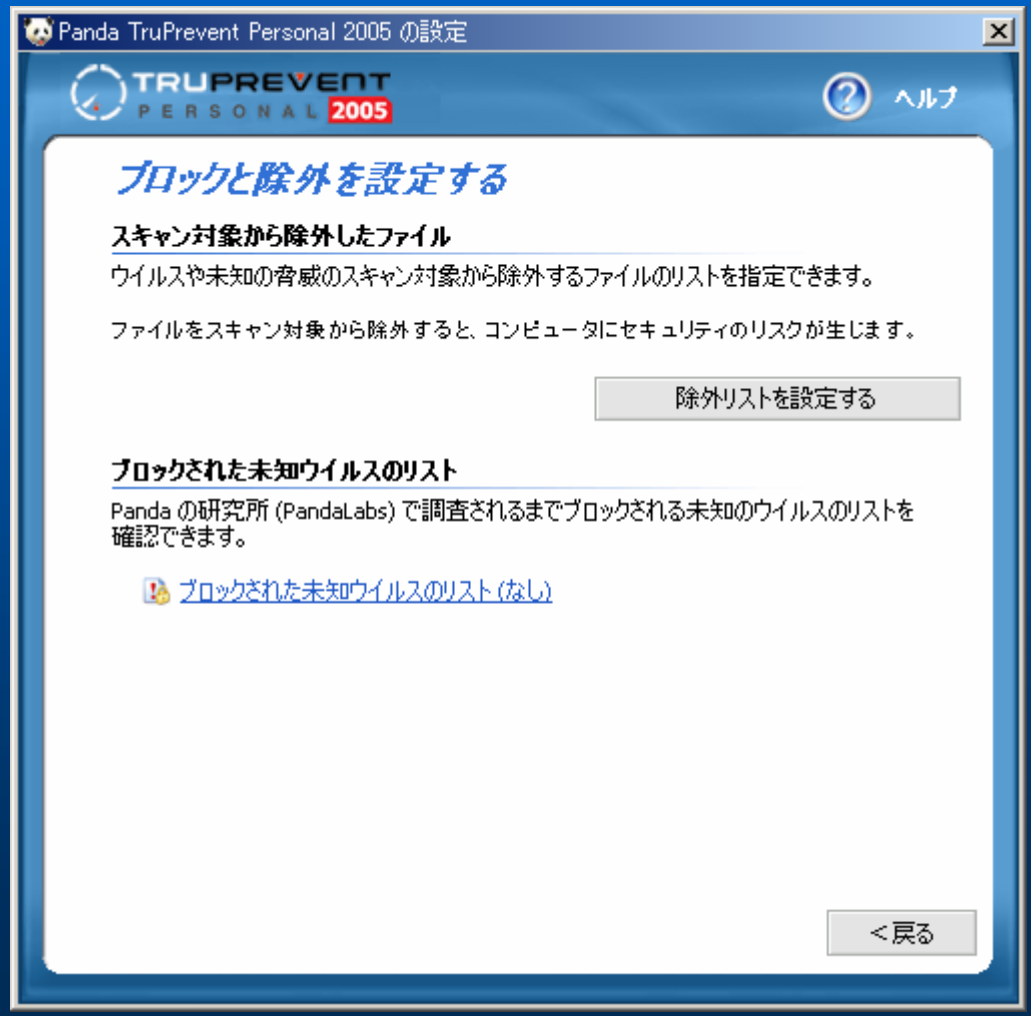
設定項目(1)

- 有効・無効くらいしかない
- それが本当は何を意味するのか不明(＾＾;;;)



設定項目(2)

- 除外設定が可能（ファイル単位）

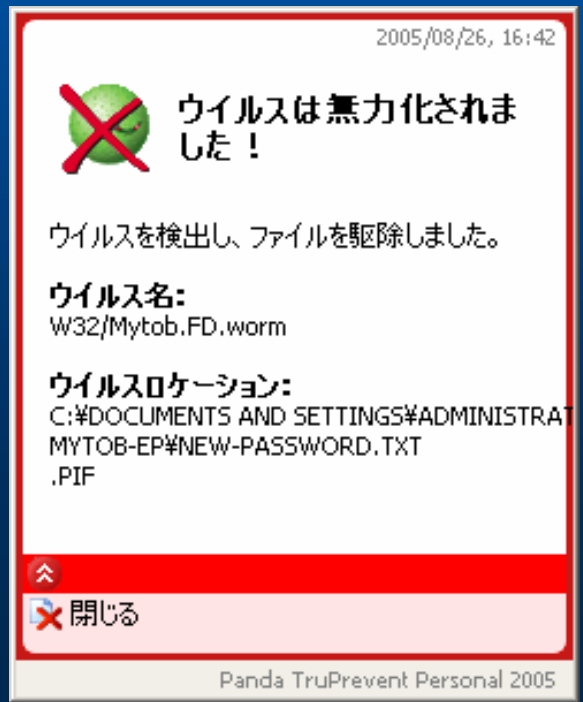


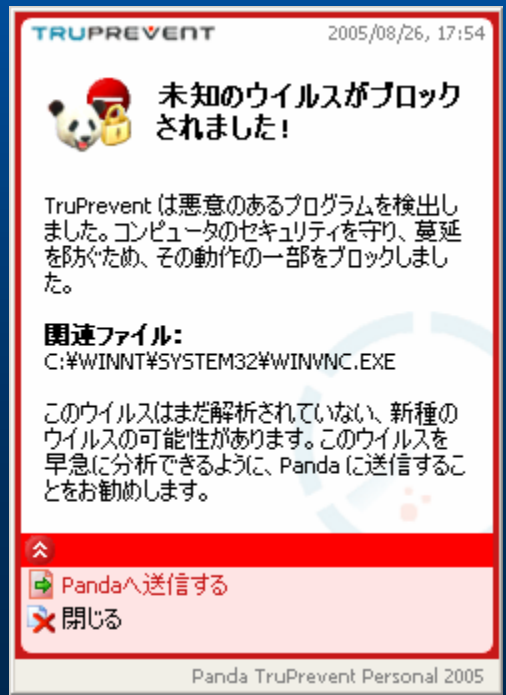
設定項目(3)

- アップデート
  - 試用版は、1 回だけアップデートできる
  - 試用版自体は 30 日間利用できる
- 何をアップデートするのか
  - どうやらウイルス定義ファイルらしい
  - TruPrevent はシグネチャ方式のチェックも実施するようだ

シグネチャマッチングの例

- Mytob-EP(Sophos 分類)を 2005-08-25 データで実行すると、W32/Mytob.FD.worm として検出・削除される
- 同じものを 2005-04-28 データ(インストール時のもの)で実行すると、未知のウイルスとして検出される(が、ある程度動作する)





なんだかうまく検出しない?

- Host-only network な VMWare 上でいくつかのウイルスを試していたのだが、なんだか検出しない事例が多いような……
- Host-only（外部との接続がない）network だから?
  - たとえば、特定のネットワーク接続を行う、ことを判断基準にしている場合にはうまく動かない可能性が
- それなりなネットワークを構築する必要がある?
- そんなときに……

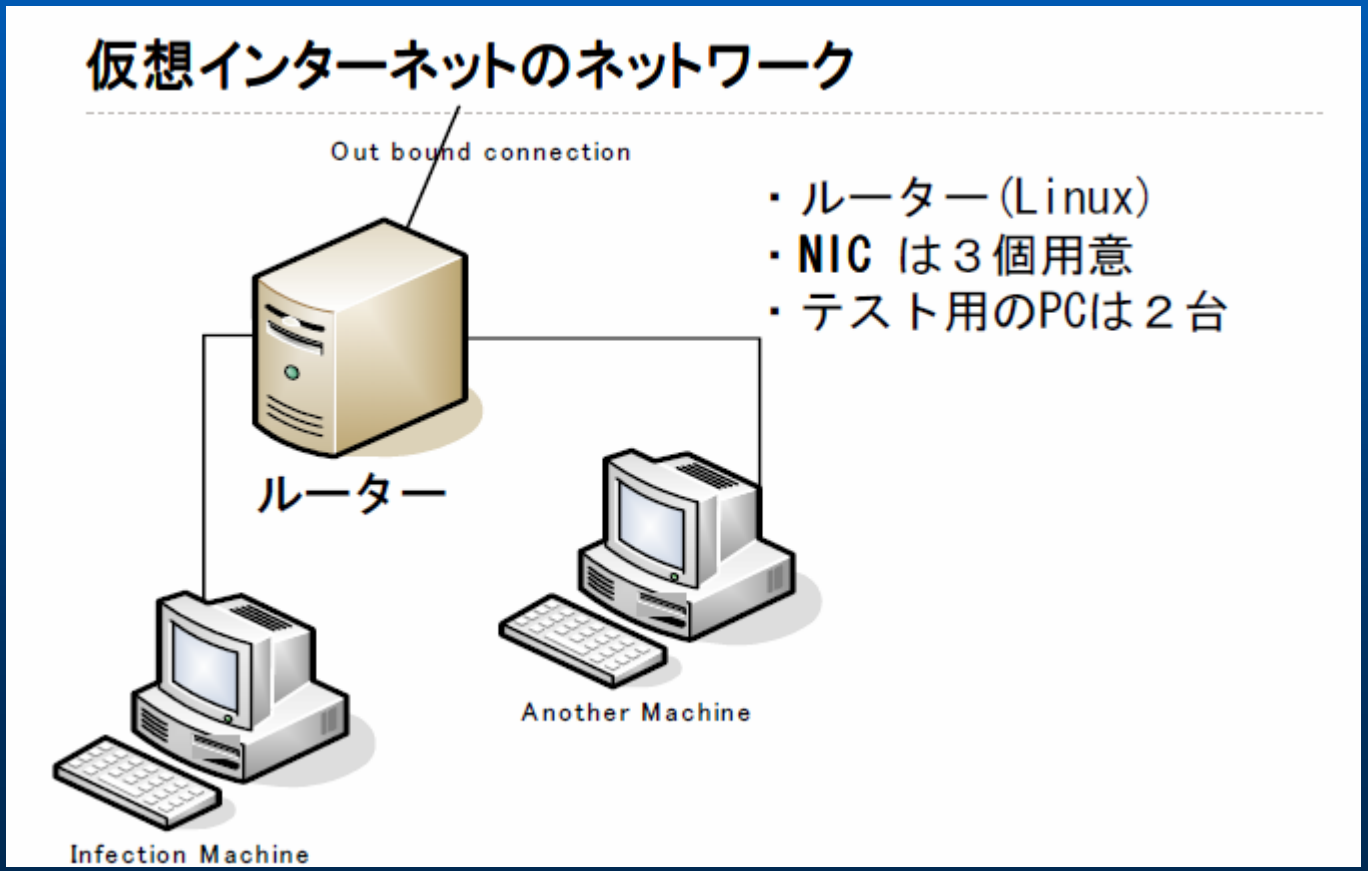
Infection Network 内での仮想インターネットの構築

- JANOG 16 で、中山 雄克 氏（シマンテック）が発表
  http://www.janog.gr.jp/meeting/janog16/abstract_01.html#abs105
  http://www.pineapple.gr.jp/JANOG16/vinet.pdf
- ウイルスなどの挙動観察用の閉鎖環境
- これをつくらないとだめなんじゃないのか?!
  ひ～

仮想インターネットの実装

仮想インターネットのネットワーク

- http://www.pineapple.gr.jp/JANOG16/vinet.pdf より引用



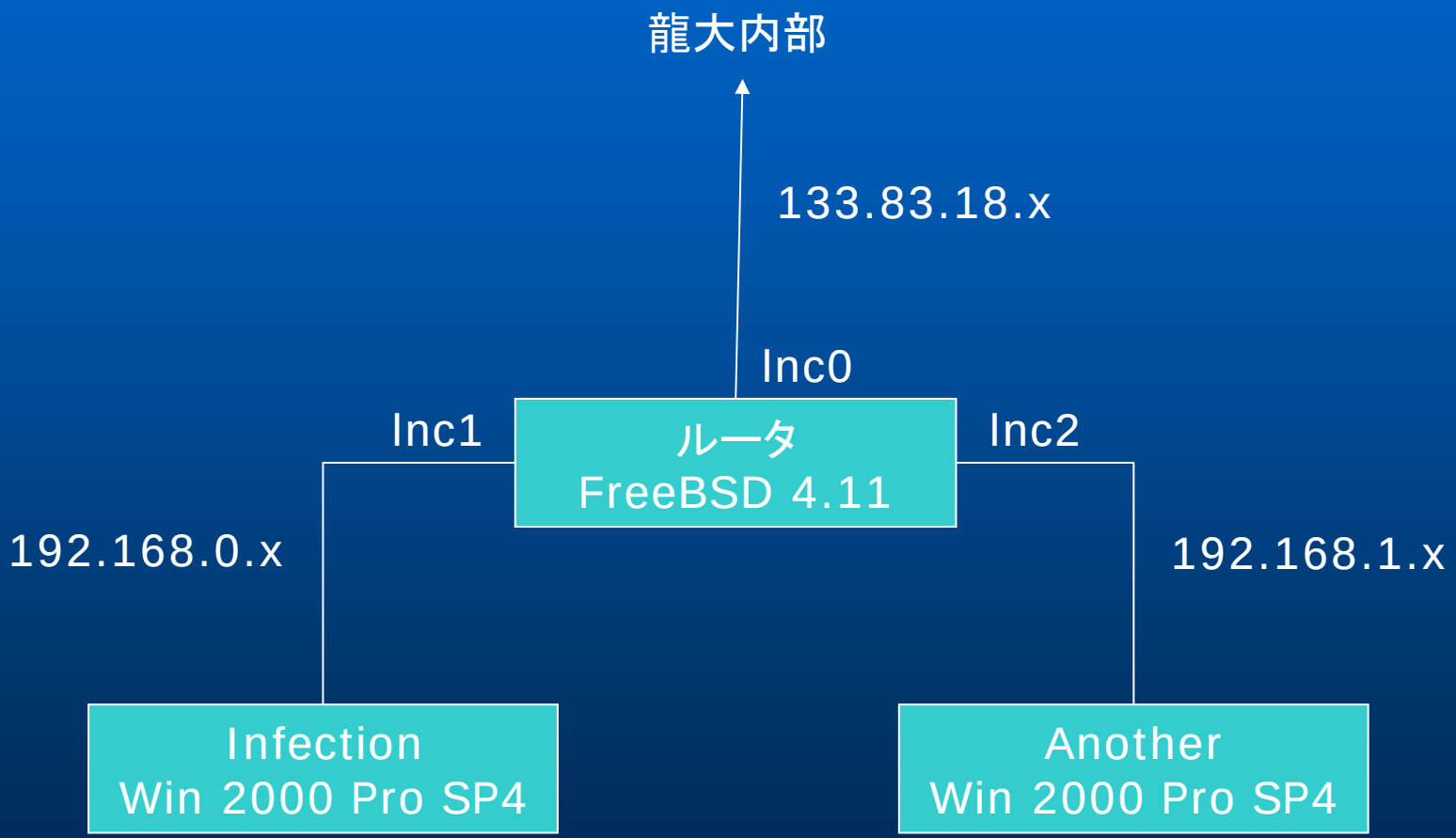
ルータ上で実現すべきこと

- DNS server を動作させ、
  - あらゆる A / MX query に対してルータの IP アドレスを返す
- web server を動作させ、
  - あらゆるリクエストに対してもエラーを返さない
  - アクセス先の URL を reply するとなおよい
- メールサーバを動作させ、
  - RCPT TO を特定の宛先に書き換えてメールを収集

ルータ上で実現すべきこと(2)

- NAT を動作させ、
  - 全パケットをルータに転送
  - Infection Machine からの攻略パケットを Another Machine に転送
  - って、なんか矛盾が(後述)
- IRC サーバ、ntp サーバ、MSN Messenger サーバ、AOL Messenger サーバを動作させる
  - MSN, AOL はシマンテック独自開発だそうだ

俺実装(1)


龍大内部
133.83.18.x
Inc0
Inc1
ルータ
FreeBSD 4.11
Inc2
192.168.0.x
192.168.1.x
Infection
Win 2000 Pro SP4
Another
Win 2000 Pro SP4

俺実装(2)

- FreeBSD 4.11-RELEASE
  - ipfilter（OS 添付）
    - ipfilter が使えるよう kernel をつくりなおし
  - bind 8(OS 添付)
  - apache 2.0.54(ports)
  - postfix 2.2.5(ports)
  - ircd

ipfilter

- NAT を動作させ、
  - 全パケットをルータに転送
  - Infection Machine からの攻略パケットを Another Machine に転送
  - って、なんか矛盾、どうするよ
- とりあえず、こうしてみた

ipfilter

/etc/ipnat.rules:

```
rdr lnc1 0.0.0.0/0 port   25 -> 133.83.18.55 port   25 tcp
rdr lnc1 0.0.0.0/0 port   80 -> 133.83.18.55 port   80 tcp

rdr lnc2 0.0.0.0/0 port   25 -> 133.83.18.55 port   25 tcp
rdr lnc2 0.0.0.0/0 port   80 -> 133.83.18.55 port   80 tcp

rdr lnc1 0.0.0.0/0 port  135 -> 192.168.1.1  port  135 tcp/udp
rdr lnc1 0.0.0.0/0 port  137 -> 192.168.1.1  port  137 tcp/udp
rdr lnc1 0.0.0.0/0 port  138 -> 192.168.1.1  port  138 tcp/udp
rdr lnc1 0.0.0.0/0 port  139 -> 192.168.1.1  port  139 tcp/udp
rdr lnc1 0.0.0.0/0 port  445 -> 192.168.1.1  port  445 tcp/udp
```

ipfilter

/etc/ipf.rules:

```
pass in     quick proto icmp from any to any
pass out    quick proto icmp from any to any
pass in     quick on lo0
pass out    quick on lo0

block in log all head 1
pass in quick proto tcp/udp from 192.168.0.0/25  to 192.168.0.0/25  keep state group 1
pass in quick proto tcp/udp from 192.168.0.0/25  to 133.83.18.55/32 keep state group 1
pass in quick proto tcp/udp from 192.168.1.0/25  to 192.168.1.0/25  keep state group 1
pass in quick proto tcp/udp from 192.168.1.0/25  to 133.83.18.55/32 keep state group 1
pass in quick proto tcp/udp from 192.168.0.0/25  to 192.168.1.0/25  keep state group 1

block out log all head 200
pass out    quick from 192.168.0.0/25  to 192.168.0.0/25 keep state group 200
pass out    quick from 133.83.18.55/32 to 192.168.0.0/25 keep state group 200
pass out    quick from 192.168.1.0/25  to 192.168.1.0/25 keep state group 200
pass out    quick from 133.83.18.55/32 to 192.168.1.0/25 keep state group 200
pass out    quick from 192.168.0.0/25  to 192.168.1.0/25 keep state group 200
```

bind 8

/etc/namedb/named.conf:

```
logging {

        channel "log_queries" {
                file "/var/log/bind/queries.log" versions 3 size 10m;
                severity info;
                print-time yes;
                print-category yes;
        };

        category queries { "log_queries"; };
};

zone "." {
        type master;
        file “root.zone";
};
```

bind 8

/etc/namedb/root.zone:

```
$TTL 86400
;
;       file : root.zone
;       zone : .
;
@               IN      SOA     tnasti-bsd    bind-admin.rins.ryukoku.ac.jp. (
                                        105081001       ; Serial
                                        10800           ; Refresh
                                        3600            ; Retry
                                        1209600         ; Expire
                                        3600            ; Minimum
                                        )

                        IN      NS      tnasti-bsd.st.ryukoku.ac.jp.
*                       IN      A       133.83.18.55
                        IN      MX      10  tnasti-bsd.st.ryukoku.ac.jp.
```

bind 8

/var/log/bind/queries.log:

```
26-Aug-2005 21:23:21.201 queries: XX+/192.168.0.1/dc21.dc21business.com/A/IN
26-Aug-2005 21:31:44.679 queries: XX+/192.168.0.1/zaminbank.net/A/IN
26-Aug-2005 21:35:58.692 queries: XX+/192.168.0.1/zajahost.net/A/IN
26-Aug-2005 21:35:58.784 queries: XX+/192.168.0.1/microsoft.com/A/IN
26-Aug-2005 21:44:31.342 queries: XX+/192.168.0.1/google.com/A/IN
26-Aug-2005 21:44:31.781 queries: XX+/192.168.0.1/www.rit.edu/A/IN
26-Aug-2005 21:44:32.222 queries: XX+/192.168.0.1/www.google.com/A/IN
26-Aug-2005 21:44:32.321 queries: XX+/192.168.0.1/www.google.com/A/IN
26-Aug-2005 21:44:48.342 queries: XX+/192.168.0.1/3.0.168.192.in-addr.arpa/PTR/IN
26-Aug-2005 21:50:29.937 queries: XX+/192.168.0.1/acs.pandasoftware.com/A/IN
26-Aug-2005 21:56:49.069 queries: XX+/192.168.0.1/www.rit.edu/A/IN
26-Aug-2005 21:56:49.165 queries: XX+/192.168.0.1/google.com/A/IN
26-Aug-2005 21:56:49.358 queries: XX+/192.168.0.1/www.google.com/A/IN
26-Aug-2005 21:57:11.741 queries: XX+/192.168.0.1/2.0.168.192.in-addr.arpa/PTR/IN
```

apache 2.0.54

/usr/local/etc/apache2/Includes/tnasti-bsd.conf:

```
RewriteEngine on

RewriteLog "/var/log/httpd-rewrite.log"
RewriteLogLevel 2

RewriteRule    ^/.*            /hoge.html      [L]

ForensicLog "/var/log/httpd-forensic.log"
```

- 「アクセス先の URL を reply するとなおよい」は実装してません

apache 2.0.54

/var/log/http-rewrite.log:

```
192.168.0.1 - - [26/Aug/2005:21:35:59 +0900]
        [zajahost.net/sid#809cdc8][rid#815d050/initial]
        (2) init rewrite engine with requested uri /c1.txt
192.168.0.1 - - [26/Aug/2005:21:35:59 +0900]
        [zajahost.net/sid#809cdc8][rid#815d050/initial]
        (2) rewrite /c1.txt -> /hoge.html
192.168.0.1 - - [26/Aug/2005:21:35:59 +0900]
        [zajahost.net/sid#809cdc8][rid#815d050/initial]
        (2) local path result: /hoge.html
192.168.0.1 - - [26/Aug/2005:21:35:59 +0900]
        [zajahost.net/sid#809cdc8][rid#815d050/initial]
        (2) prefixed with document_root to
        /usr/local/www/data/hoge.html
192.168.0.1 - - [26/Aug/2005:21:35:59 +0900]
        [zajahost.net/sid#809cdc8][rid#815d050/initial]
        (1) go-ahead with /usr/local/www/data/hoge.html [OK]
```

apache 2.0.54

/var/log/httpd-forensic.log の例:

```
+VC3p1YVTEjcAABGVfzQAAAAH|GET /ftp/file.exe HTTP/1.1|User-Agent:
        Mozilla/5.0|Host:zaminbank.net
-VC3p1YVTEjcAABGVfzQAAAAH
+Y0--loVTEjcAABFyHCwAAAAB|GET /c1.txt HTTP/1.1|User-Agent:
        Mozilla/5.0|Host:zajahost.net
-Y0--loVTEjcAABFyHCwAAAAB
```

- mod_forensic は ports 標準では構成されないので注意
  - Makefile.modules の MISC_MODULES= に log_forensic を追加
  - (Makefile の CONFIGURE_ARGS= に --enable-log-forensic を追加)
  - log_forensic を使うには mod_uniqid も必要だが、これはデフォルトで入っているようだ

postfix 2.2.5

/usr/local/etc/postfix/main.cf:

```
recipient_canonical_maps =
        pcre:/usr/local/etc/postfix/recipient_canonical.txt
```

/usr/local/etc/postfix/recipient_canonical.txt:

```
/^.*$/  root@tnasti-bsd.st.ryukoku.ac.jp
```

ircd やら IM やら

- irc2.10.3p7+jp6 をインストールしてみたが、なんだかうまく動いていないようだ
  - 俺のスキル不足 orz
- IM ものは独自実装が必要だが
  - 俺のスキル不足 orz

- 麻薬もたしなまないとだめですか、そうですか。

Windows 2000 SP4

- ふつうの Windows 2000 SP4 + IE6 SP1
- てきとうなメールアカウントをつくっておく
- 状況監視ツール
  - sysinternals.com の Process Explorer と TCP View をインストール
    - タスクマネージャや cmd.com はウイルスによって強制終了させられることが多い
  - Startup Control Panel と Startup Monitor をインストール
    http://www.mlin.net/StartupCPL.shtml
    http://www.mlin.net/StartupMonitor.shtml
  - hosts ファイル監視用にファイル監視をインストール
    http://www.vector.co.jp/soft/win95/util/se132799.html

やってみました

デモ　orz

Panda TruPrevent
調査結果

TruPrevent 調査結果

- パターンに該当すればウイルスとして検出
- パターンに該当しない場合は、ウイルスには感染してしまう
  - C:¥WINNT¥System32¥ とかに保存されてしまう
  - hosts ファイルやレジストリ (HKLM / Run とか)も改変されてしまう
- mass mailing 型のウイルスについては検出してくれるようだが、検出されるまでにいくつかメールが送られてしまう場合がある
- ダウンローダは?
  - ダウンロードしたものに依存すると思われ
- ネットワーク感染型については?
  - Mytob-EF での状況を見ると期待できない?

今後の予定

- 仮想インターネットの改良
  - 特に irc 方面
- いろいろなウイルスでの TruPrevent のテスト
  - 誰か検体ください（Zotob とか……）
- 他社のもののテスト
  - Cisco Security Agent
  - eEye Blink