

VMKnoppix 20080827 版 (KNOPPIX5.3.1 ベース。DVD サイズ)

VMKnoppix は多くの仮想計算機ソフトウェアを使いやすく収録した 1 DVD Linux(KNOPPIX)です。

<http://www.rcis.aist.go.jp/project/knoppix/vmknoppix/index.html>

■ この版の特徴

- **Virtual TPM** を **Xen, KVM/QEMU** で利用可能にしました。この仮想マシン上で上記の **Trusted Computing** が確認できます。
- **Trusted Computing** が確認できる実行環境(Trusted GRUB, Linux-IMA kernel, TrouSerS, OpenPTS など。以前 **KNOPPIX for Trusted Computing Geeks** と呼ばれていたもの)を含めました。
- TPM の状態が確認できる **TPM Checker** を加えました。
- **FailSafe-C, vx32, LLVM(Low Level Virtual Machine)**などセキュリティおよび最適化に関するコンパイラを含めました。
- 仮想マシンモニタの **BitVisor 0.3** を収録しました。
- インターネットブートローダの **InetBoot** を収録しました。
 - GRUB メニューから古い VMKnoppix/Xenoppix をインターネット起動できます。
- ネットワークブートローダの **gPXE** を収録しました。ネットワークからカーネル、ミニルートを取得して起動できます。
- インターネットクライアントの **OS Circular** により、仮想計算機{Xen|QEMU|KQEMU|KVM}上で各種 Linux {CentOS5|Debian Etch|Ubuntu606|Ubuntu610|Ubuntu704}がネットワーク仮想ディスク (Trusted HTTP-FUSE CLOOP)から起動します。

下記の仮想計算機ソフトウェアが収録されています。

- Xen3.2.1 (Dom0 kernel 2.6.18) <http://www.cl.cam.ac.uk/research/srg/netos/xen/>
- BitVisor0.3 <http://www.securevm.org/bitvisor.html>
- KVM60 <http://sourceforge.net/projects/kvm>
- QEMU091 <http://fabrice.bellard.free.fr/qemu/>
- KQEMU <http://fabrice.bellard.free.fr/qemu/kqemu-doc.html>
- UML <http://user-mode-linux.sourceforge.net/>
- Virtual Box <http://www.virtualbox.org/>

下記のネットワークブートソフトウェアが収録されています。

- gPXE <http://www.etherboot.org>
- InetBoot <http://openlab.jp/oscircular/inetboot/>
- OSCircular <http://openlab.jp/oscircular>

下記のセキュリティおよび最適化に関するコンパイラが収録されています。

- FailSafe-C <http://www.rcis.aist.go.jp/project/FailSafeC-ja.html>
- VX32 <http://pdos.csail.mit.edu/~baford/vm/>
- LLVM <http://llvm.org/>

ダウンロード

- ファイル名: knoppix_v5.3.1DVD20080326_xen3.2.1-20080827.iso (MD5: bdf1ef34a688cef1e378919acbedccdf)
- FTP: (Ring Servers): ftp://ring.aist.go.jp/archives/linux/knoppix/iso/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso
- HTTP (Ring Servers): http://ring.aist.go.jp/archives/linux/knoppix/iso/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso
- Bittorrent: http://www.rcis.aist.go.jp/project/knoppix/download/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso.torrent

使い方目次

1	VMKnoppix の起動方法	3
2	仮想化ソフトウェアの使い方	4
2.1	Xen	4
2.1.1	Xen 3.2.1 の DomainU/HVM-Domain の使い方	4
2.1.2	Xen-HVM による Virtual TPM の使い方	4
2.2	KVM, KQEMU, QEMU	5
2.2.1	KVM/QEMU による Virtual TPM の使い方	5
2.2.2	Virtual TPM のまとめ	5
2.2.3	QEMU x86_64 (AMD-V)の使い方	6
2.3	VirtualBox	6
2.4	UML (UserMode Linux)	6
2.5	BitVisor 0.3	6
2.5.1	起動方法	6
2.5.2	確認方法	7
3	ネットワークブート	8
3.1	InetBoot	8
3.2	gPXE	8
3.2.1	gPXE による HTTP-FUSE KNOPPIX の起動	8
3.2.2	gPXE と BitVisor の組合せ	9
3.3	OS Circular	9
3.3.1	通常カーネルで起動した場合	9
3.3.2	Xen3.2.1 で起動した場合	10
3.3.3	インターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)単体のマウント	10
3.3.4	インターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)の負荷分散	11
4	Trusted Computing (旧 KNOPPIX for Trusted Computing Geeks)	12
4.1	収録ソフトウェア	12
4.2	使い方	12
4.2.1	iceweasel をアップデートしなかった場合	12
4.2.2	iceweasel をアップデートする場合	13
5	コンパイラ関係	17
5.1	FailSafe-C	17
5.2	VX32	17
5.3	LLVM (Low Level Virtual Machine)	17
6	全体に関する関連論文/発表	18

1 VMKnoppix の起動方法

VMKnoppix はブートローダに GRUB-IMA を採用し、Trusted Boot により TPM/BIOS-ACPI に起動ログを残します。下図は表示される GRUB メニューです。

```
GNU GRUB version 0.97-ima-1.1.0.0 (638K low
KNOPPIX 5.3.1(normal kernel)
KNOPPIX/Xen3.2.1
KNOPPIX 5.3.1(normal kernel+ima)
BitVisor 0.3
boot from hd0
gPXE
TPM Checker
InetBoot-netfs VMKnoppix(Xen3.2.0)
InetBoot-netfs VMKnoppix(Xen3.1.1)
InetBoot-netfs VMKnoppix(Xen3.1.0)
InetBoot-netfs VMKnoppix(Xen3.0.4.1) Oprofile
InetBoot-netfs VMKnoppix(Xen3.0.4.0)
```

起動メニューの内容

GRUB メニュー	用途
KNOPPIX 5.3.1 (normal kernel)	通常の KNOPPIX(Linux 2.6.24)として起動します。
KNOPPIX/Xen 3.2.1	Xen3.2.1 + Linux 2.6.18 で起動します。
KNOPPIX 5.3.1 (normal kernel + ima)	GRUB-IMA&Linux2.6.24-IMA により Trusted Boot をします。起動の完全性およびパッケージの脆弱性を OpenPTS により確認できます。
BitVisor 0.3	BitVisor を Intel VT で起動・挿入し、GRUB メニューに戻ります。
boot from hd	ハードディスク上の OS を起動。
gPXE	ネットワークブート。PXE ブートおよび HTTP からの起動
TPM Checker	TCG-BIOS の機能を確認します。
InetBoot-netfs	ネットワーク上の VMKnoppix ISO ファイルからの起動
InetBoot-HTTP-FUSE	HTTP-FUSE VMKnoppix の起動。GuestOS は Plan9,NetBSD
BuidRoot Shell	InetBoot が使っている BuildRoot の shell 起動

➤ eth0 が利用できることを確認してください。DHCP は下記コマンドを実行してください。

pump -i eth0

☆ IEEE1394 が使える PC (Intel Mac など)では nofirewire をカーネルオプション(GRUB の 2 行目)につけてください。

2 仮想化ソフトウェアの使い方

個々の仮想ソフトウェアの使い方を紹介します。

2.1 Xen

GRUB メニューで KNOPPIX/Xen 3.2.1 を選択して起動してください。

2.1.1 Xen 3.2.1 の DomainU/HVM-Domain の使い方

VMKnoppix では起動のために簡単コマンドを用意しています。

- ◇ DomainU で VMKnoppix DVD イメージを起動します。

knoppixU

- ◇ HVM Domain (IntelVT あるいは AMD-V が必要)で VMKnoppix DVD イメージを起動します。

knoppixHVM

デフォルトでは、VMKnoppix の DVD イメージから起動しますが、他の 1CD/DVD OS の ISO ファイルもオプション(<http://URL> または <file://絶対ディレクトリ>)で渡すことができます。

#knoppixHVM http://example.com/knoppix/*.iso**

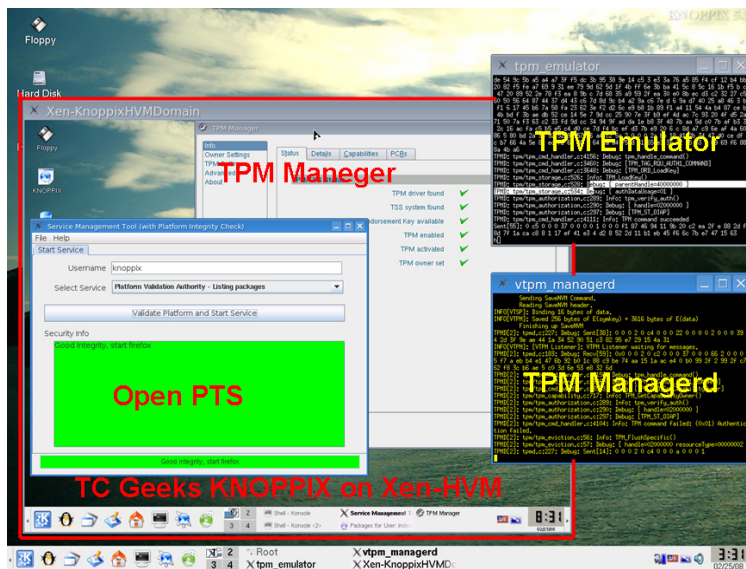
#knoppixHVM file://home/knoppix/*.iso**

2.1.2 Xen-HVM による Virtual TPM の使い方

Virtual TPM(TPM Emulator)をまず最初に起動してください。

xen_vtpm start

“tpm_emulator” と “tpm_mangerd” の 2 つのウィンドウが開きます。もし、片方のみの場合は `xen_vtpm stop` で終了して、再度 `xen_vtpm start` を実行してください。



この後は、通常版と同じです。knoppixHVM あるいは knoppixU で tpm が使えます。TPM の動作を確認するには、KNOPPIX for Trusted Computing Geeks をお勧めします。ISO ファイルを指定して下記のように実行できます。

#knoppixHVM http://example.com/knoppix/knoppix511-TC-Geeks-100.iso

#knoppixHVM file://tmp/knoppix511-TC-Geeks-100.iso

2.2 KVM, KQEMU, QEMU

GURB メニューで KNOPPIX 5.3.1 (normal kernel)で起動してください。下記のコマンドは自動的に KVM,KQEMU,QEMU 環境を認識して適するドライバを組み込みます。KVM あるいは KQEMU, QEMU 上で VMKnoppix DVD イメージを起動します。

```
# qemu-knoppix.sh
```

オプション “-no-kvm” KVM カーネルモジュールの組込みをキャンセルします。

“-no-kqemu” KQEMU カーネルモジュールの組込みをキャンセルします。

“-no-module” カーネルモジュールの組込みをキャンセルします。

“-tpm” Virtual TPM を有効にして起動します。

ISO ファイルを指定して下記のように実行できます。

```
# qemu-knoppix.sh http://example.com/knoppix/knoppix.iso
```

```
# qemu-knoppix.sh file://tmp/knoppix.iso
```

注意点:

KVM を起動する場合には GuestOS の GRUB で “**nolapic**” オプションを追加してください。

2.2.1 KVM/QEMU による Virtual TPM の使い方

“qemu-knoppix.sh”スクリプトでは “-tpm”オプションにより、Virtual TPM が有効になります。

```
# qemu-knoppix.sh -tpm
```

VMKnoppix DVD のイメージで起動するので、GRUB メニューから”KNOPPIX 5.3.1 (normal kernel + ima)”を選択してください。

KVM コマンド単体から起動する場合は事前に tpmcmd コマンドを実行して下さい。

```
# tpmcmd clear
```

```
# kvm -m 512 -no-kvm-irqchip -L /usr/share/tcgbios -cdrom /dev/cdrom
```

Intel-VT/ADM-V がない場合あるいは無効にした場合でも virtual TPM は利用できます。ただし、この場合は QEMU として動くのでかなり遅くなります。

```
# rmmod kvm
```

```
# rmmod kvm-intel
```

```
# tpmcmd clear
```

```
# kvm -m 512 -no-kvm-irqchip -L /usr/share/tcgbios -cdrom /dev/cdrom
```

2.2.2 Virtual TPM のまとめ

特徴をまとめると下記の表になります。赤字が問題点です。

	Xen-HVM	KVM	QEMU(KVM から起動)
ホスト環境	Dom0 カーネルが Linux2.6.18 に固定。ドライバに制限あり。	ホストのカーネルは任意。最新のドライバが使える。	ホストのカーネルは任意。最新のドライバが使える。
CPU	Intel VT あるいは AMD-V が必要	Intel VT あるいは AMD-V が必要	CPU に制限なし。
性能	早い	早い	遅い

Virtual TPM に関する発表を Virtualization Mini Summit at Ottawa Linux Symposium 2008 で行いましたのでこちらのスライド資料も参考にして下さい。

Virtual TPM on Xen/KVM for Trusted Computing

2.2.3 QEMU x86_64 (AMD-V)の使い方

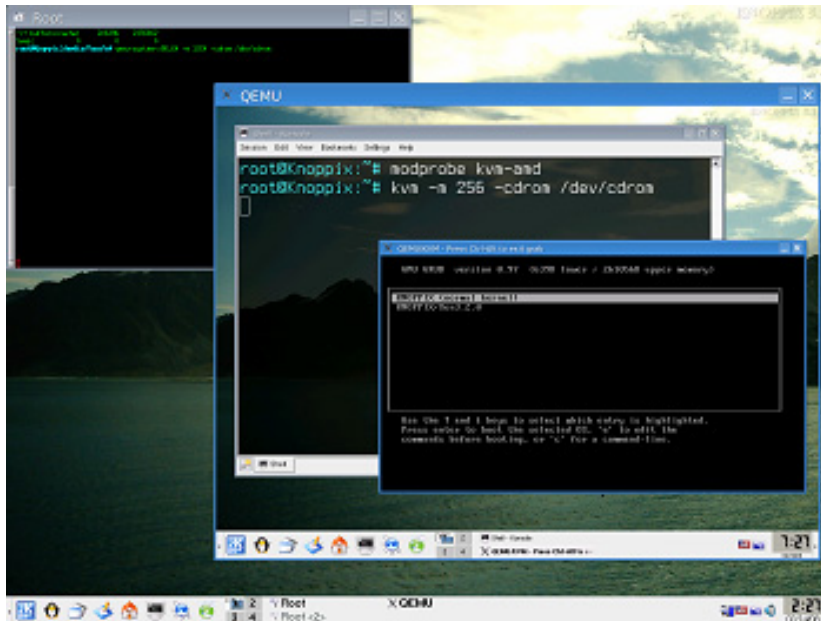
QEMU x86_64 は AMD-V 命令をエミュレートしており、この上で KVM などの仮想化が使えます。残念ながら Xen は動きません。

```
# qemu-system-x86_64 -m 512 -cdrom /dev/cdrom
```

この仮想マシンの上で KVM を実行することができます。

```
# kvm -m 512 -cdrom /dev/cdrom
```

GuestOS の GRUB で “**nolapic**” オプションを追加してください。



2.3 VirtualBox

GRUB メニューで KNOPPIX 5.3.1 (normal kernel) で起動してください。下記のコマンドで VirtualBox の実行環境をセットアップします。

```
# modprobe vboxdrv
```

```
# virtualbox
```

2.4 UML (UserMode Linux)

GRUB メニューで KNOPPIX 5.3.1 (normal kernel) で起動してください。下記のコマンドで UML が VNC 上に KNOPPIX を起動します。

```
# umlknx.sh
```

2.5 BitVisor 0.3

BitVisor は Intel VT で稼動する仮想マシンモニタです。Windows のセキュリティを強化するために開発された国産の仮想マシンモニタです。現在、提供している BitVisor0.3 はコアのみなので特別な機能はありませんが、簡単なインストールだけできます。

2.5.1 起動方法

GRUB メニューで BitVosr を選択してください。BitVisor が Intel VT の root mode でインストールされ、GRUB にメニューが戻ってきます。その後、好きな OS を GRUB メニューから選択してください。non-root

mode で OS が起動します。

ハードディスクに入っている OS の起動は GRUB メニューの bootfrom hd0 でできます。デフォルトでは第一パーティションに入っている OS を起動します。別のパーティションに OS があれば、GRUB メニューで rootnoverify hd(0,0)になっている部分を hd(0,1)などに変えてください。2 番目に数字はパーティションの番号を示しています。Windows がインストールされていれば BitVisor 上で Windows が起動します。

GRUB メニューで KNOPPIX5.3.1 を選択すれば BitVisor 上で KNOPPIX も起動します。Xen は BitVisor が root mode にインストールされているため起動できません。

gPXE と組み合わせてネットワークブートもできます。

2.5.2 確認方法

F12 キーを押すとシリアルコンソールに”F12 Pressed”のメッセージで現れ、BitVisor が入っていることが確認できます。この動作はシリアルコンソールのみで Windows や X Window からは確認できません。

VMKnoppix では GRUB-IMA による Trusted Boot を行なっているため、TPM と BIOS の ACPI に起動ログが残っています。KNOPPIX で TPM モジュールを組み込むことでその存在 (BitVisor の SHA1 値) が確認できます。

```
# sha1sum /cdrom/boot/isolinux/bitvisor.elf
```

```
aa28a31eeda42585813dd3d6f7be3fd117b69fcf /cdrom/boot/isolinux/bitvisor.elf
```

```
# modprobe tpm_tis
```

```
# mount -t securityfs none /sys/kernel/security
```

```
# cat /sys/kernel/security/tpm0/ascii_runtime_mesurements
```

```
4 89f0284e00992d067654818a9f2c09bbaa31acde 05 [Booting CD ROM, - MATSHITADVD-RAM UJ-833S]
4 19d1733e8f9645c090f8fce58a7f943a30fbc66 0d [IPL]
4 ec2afa621c866fd0c128d309e2415a4f49262acb 0d [IPL]
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 bc74830d55c1cff5603df9ff93387b51d5db9f68 0e [IPL Partition Data]
5 d63d12ced978aca120bfe6ee7683e394c2ffaef0 05 [Boot Sequence User Intervention]
5 371436a31b138be9f75b887f02b9bd723cc21e4c 1105 []
8 aa28a31eeda42585813dd3d6f7be3fd117b69fcf 1205 [] /** BitVisor **/
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 be25adb01778393bbcae98ee871528fabfc85902 1005 []
4 ec2afa621c866fd0c128d309e2415a4f49262acb 0d [IPL]
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 bc74830d55c1cff5603df9ff93387b51d5db9f68 0e [IPL Partition Data]
5 646b02b443f710cfb55debe234070588978828e5 1105 []
8 3efcce6615807a884992b9555f0a311fb8b474a6 1205 []
8 5c6e6c260a2d674fa13f5115b7eaf5499733e3f9 1405 []
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []
```

3 ネットワークブート

VMKnoppix に収録されている 3 種類のネットワークブート(InetBoot, gPXE, OSCircular)について説明します。

3.1 InetBoot

InetBoot は Internet 上に公開されているハイパーバイザー、カーネル、ミニルートをダウンロードし、**kexec** で起動(Warm Boot)するブートローダです。InetBoot の実態は小さい Linux である **BuildRoot** です。BuildRoot 内でネットワークの設定やカーネルの取得などを行い、kexec により Warm Boot します。つまり、目的の OS 起動の前に各種の操作を行なえる**プレブート(PreBoot)機能**を有しています。GRUB メニューの BuildRoot Shell でプレブートの実行環境を確認できます。

ディスクイメージ取得方法に **NetFS 版**と **HTTP-FUSE 版**があります。NetFS 版では httpfs を使って HTTP サーバ上の KNOPPIX ISO ファイルを利用します。HTTP-FUSE 版では公開されているインターネット仮想ディスク”HTTP-FUSE CLOOP”をルートファイルシステムとして起動します。

VMKnoppix に収録したものは GRUB メニューから選択するのみです。ネットワークカードの種類によって起動できないものもあります。

3.2 gPXE

gPXE はネットワークブートローダです。デフォルトでハードウェアの PXE と同様に TFTP ブートします。コマンドを加えることで HTTP や iSCSI から起動することも出来ます。

3.2.1 gPXE による HTTP-FUSE KNOPPIX の起動

gPXE 起動後はデフォルトで TFTP ブートに移ります。その前に **CTL+B** でシェルに落ちます。シェルで下記コマンドを実行してください。

```
gPXE> dhcp net0
gPXE> kernel http://www.inetboot.net/knoppix511.gpxe
gPXE> boot
```

最初のコマンドは DHCP による IP アドレス設定です。ネットワークカードによっては設定できないことがあります。この場合、gPXE は使えません。

IP アドレスの設定が出来れば、gPXE に HTTP-FUSE KNOPPIX 起動するスクリプトをダウンロードしてください。最後に boot コマンドで起動します。この後は通常の HTTP-FUSE KNOPPIX が起動します。

```
ISOLINUX 3.11 2005-09-02 Copyright (C) 1994-2005 H. Peter Anvin
Etherboot ISO boot image generated by geniso
Loading gpxe.krn.....Ready.
pcnet32.c: Found pcnet32, Vendor=0x1022 Device=0x2000
10Mbps Full-Duplex
WARNING: Using legacy NIC wrapper on 00:0c:29:69:66:7d

gPXE 0.9.3 -- Open Source Boot Firmware -- http://etherboot.org
Features: HTTP DNS TFTP iSCSI AoE bzImage Multiboot NBI PXE PXEXT
Press Ctrl-B for the gPXE command line..._
```

```
gPXE> dhcp net0
DHCP (net0 {  
gPXE> kernel http://www.inetboot.net/knoppix511.gpxe
http://www.inetboot.net/knoppix511.gpxe... ok
gPXE> boot
http://knoppix.inetboot.net/archives/linux/oscircular/tcgeeks/v1.0/linux... _
```

上記の例は KNOPPIX5.1.1 を起動しますが、2行目の URL は下記に変えれば 5.0.1, 4.0.2, 他を起動できます。

- ◆ <http://www.inetboot.net/knoppix501.gpxe>
- ◆ <http://www.inetboot.net/knoppix402.gpxe>
- ◆ <http://www.inetboot.net/gpxe/fedora9>
- ◆ <http://www.inetboot.net/gpxe/fedora8>
- ◆ http://www.inetboot.net/gpxe/fedora9-x86_64
- ◆ http://www.inetboot.net/gpxe/fedora8-x86_64
- ◆ <http://www.inetboot.net/gpxe/ubuntu804>
- ◆ <http://www.inetboot.net/gpxe/ubuntu710>
- ◆ http://www.inetboot.net/gpxe/ubuntu804-x86_64
- ◆ <http://www.inetboot.net/gpxe/knoppix531-remasterCD>
- ◆ <http://www.inetboot.net/gpxe/vmknoppix-xen321>

3.2.2 gPXE と BitVisor の組合せ

gPXE は BitVisor のロード後でも利用可能です。BitVisor 上で TFTP ブートや HTTP-FUSE KNOPPIX が動きます。この場合、起動した OS は Intel VT の non-root モードで起動していることとなります。

3.3 OS Circular

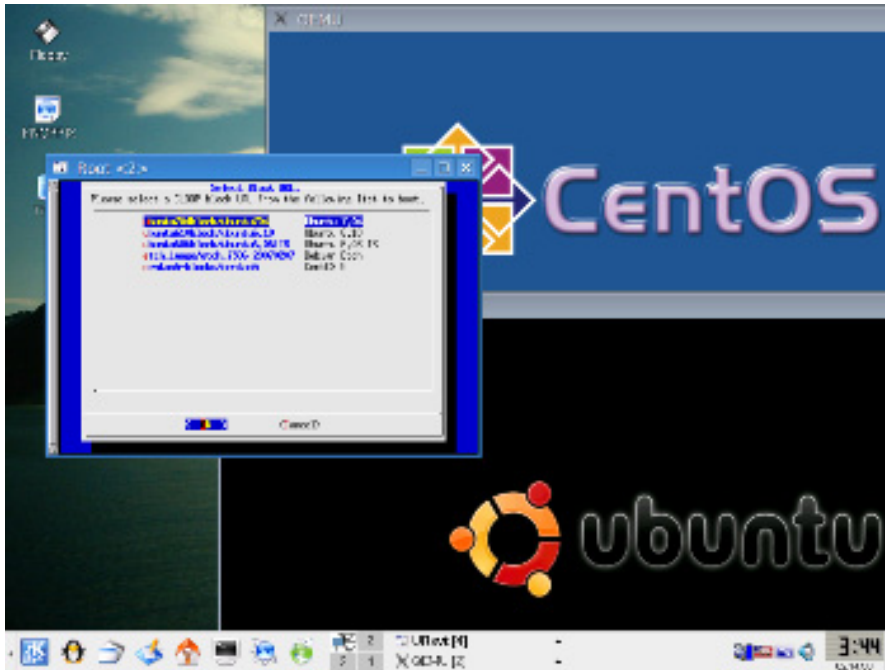
インターネット上のディスクイメージから仮想マシンを起動します。

3.3.1 通常カーネルで起動した場合

KVM, KQEMU, QEMU でインターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)が使えます。それぞれのコマンドを実行すると仮想ディスク使って VM が起動します。

```
#httpfuse-kvm
#httpfuse-kqemu
#httpfuse-qemu
```

選択メニューが出ますので、起動したい OS を選んでください。Account/Password はすべて http-fuse/http-fuse になっています。



3.3.2 Xen3.2.1 で起動した場合

Xen-HVM でインターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)が使えます。まず、ネットワークと Xen 環境を整備してください。

```
# pump -i eth0
```

```
# /etc/init.d/xend start
```

下記コマンドを実行すると仮想ディスク使って Xen-HVM が起動します。

```
#httpfuse-hvm
```

選択メニューが出ますので、起動したい OS を選んでください。Account/Password はすべて http-fuse/http-fuse になっています。

3.3.3 インターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)単体のマウント

まずインターネット仮想ディスクを設定するため、マウントポイントなどを整備します。

```
# mkdir /var/tmp/blocks
```

下記のマウントポイントは任意。

```
# mkdir /media/thfc
```

```
# mkdir /media/guestos
```

MappingTable ファイルをダウンロードします。MappingTable ファイルは下記の URL よりダウンロードできます。

<http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx>

http://vmimage.inetboot.net/archives/linux/oscircular/pc/etch_image/etch_i386-20070207.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/etch_image/etch_i386-20061221.idx

<http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu606block/ubuntu6.06LTS.idx>

<http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu610block/ubuntu6.10.idx>

<http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu704block/ubuntu704.idx>

下記に CentOS を例にルートファイルシステムの取り出し方を示します。

```
# cd /var/tmp/blocks/  
# wget http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx  
# httpstorged -f ¥  
  /media/htfs http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx
```

以上で /media/thfc/centos5 という仮想ファイルができます。

これはハードディスクイメージになっているため、取扱いが多少面倒です。

```
# losetup /dev/loop0 /mountpoint/centos5  
# kpartx -a /dev/loop0
```

とすると、 /dev/mapper/ 以下に loop0p1 (/boot), loop0p2 というノードができます。loop0p2 は lvm partition なので、

```
# lvmdiskscan  
# vgchange -a y
```

とすると、ようやく /dev/VolGroup00/LogVol00 というデバイスノード(CentOS の /)ができます。これをマウントするとゲスト OS のルートファイルシステムが現れます。

```
#mount /dev/VolGroup00/LogVol00 /media/guestos
```

3.3.4 インターネット仮想ディスク(Trusted HTTP-FUSE CLOOP)の負荷分散

Trusted HTTP-FUSE CLOOP は細かいブロックファイルから 1 つの仮想ディスクを構築します。ブロックファイルは HTTP サーバからダウンロードしますが、遠距離のサーバからだとネットワーク遅延により非常に遅くなります。現在、アメリカに 3 サイト、ヨーロッパに 3 サイト、日本(ring サーバ)約 7 サイトを配置し、もっと近いサーバを DNS-Balance により自動的に見つけるようになっています。ご興味のある方はダウンロードの様子を調べるとサーバが変わることが確認できます。

4 Trusted Computing (旧 KNOPPIX for Trusted Computing Geeks)

この KNOPPIX では OpenPlatformTrustedServices を収録し、実証実験を行なっているリモートアテステーションによる第三者検証ができます。

リモートアテステーションにより「正しい起動が行なわれていること」の**構成検証**と「利用しているパッケージに脆弱性がないこと」の**脆弱性検証**ができます。現在の脆弱性情報は DSA: Debian Security Advisory から作成され、起動後に正しい Debian パッケージが使われているか検証できます。

この機能は Xen-HVM, KVM, QEMU で提供されている Virtual TPM で動作確認ができます。

4.1 収録ソフトウェア

- ◆ GRUB-IMA1.1.0.0
 - <http://trousers.sourceforge.net/grub.html>
- ◆ kernel 2.6.24+IMA(Integrity Measurement Architecture)
 - <http://sourceforge.net/projects/linux-ima>
- ◆ Trousers0.3.1
 - <http://trousers.sourceforge.net/>
- ◆ TPM_Manager0.5
 - <http://sourceforge.net/projects/tpmmanager>
- ◆ OpenPTS v0.1.2 (Platform Trusted Services)
 - <http://sourceforge.jp/projects/openpts/>

4.2 使い方

下記の手順で OpenPTS を使ったりリモートアテステーションの構成検証と脆弱性検証ができます。旧 KNOPPIX for Trusted Computing Geeks ではグラフィカルインターフェースがありましたが、現在はコマンドラインで利用できるようになっています。

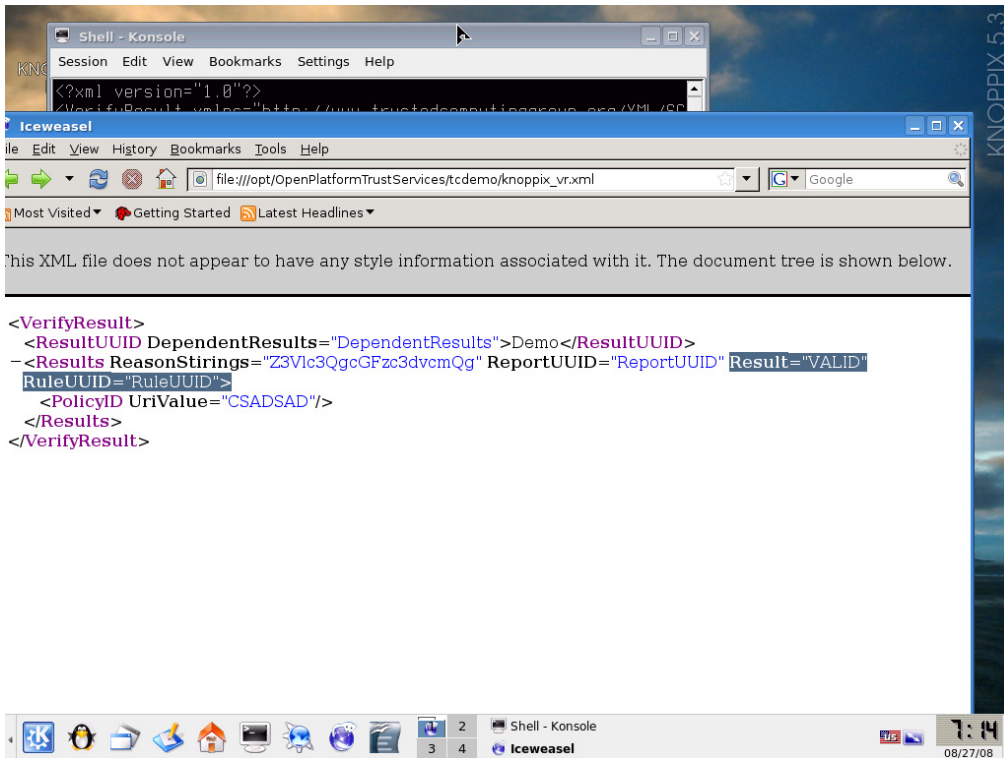
デフォルトでは iceweasel 2.0.0.12-1 に脆弱性があり、脆弱性検証が失敗する設定になっています。iceweasel 3.0.1-1 にをアップデートすれば脆弱性検証が成功します。

4.2.1 iceweasel をアップデートしなかった場合

下記の例ではユーザを knoppix にしましたが、ユーザ名は任意です。

```
# mount -t securityfs none /sys/kernel/security/
# tcspd
# tpm_takeownership
Enter owner password: knoppix
Confirm password: knoppix
Enter SRK password: (Just Return)
Confirm password: (Just Return)

# cp /opt/OpenPlatformTrustServices/tcdemo/dummy_system.data /var/lib/tpm/system.data
cp: overwrite `var/lib/tpm/system.data'? yes
```

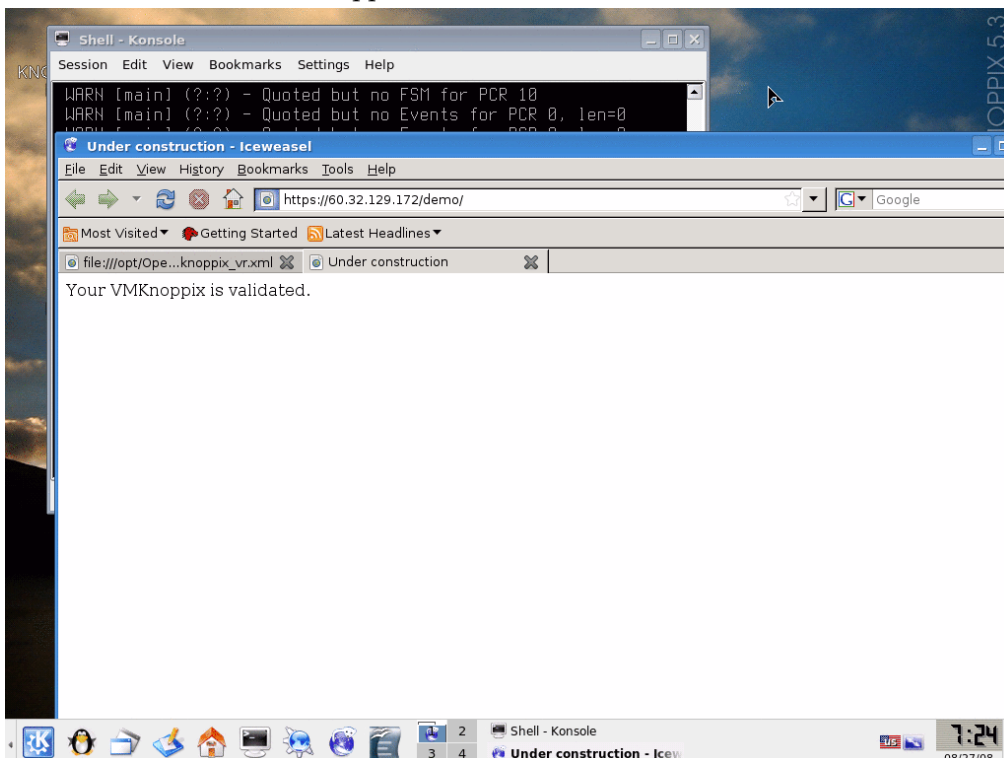
また、ブラウザが立ち上がります。現状では Secure Connection が Fail しますが、iceweasel で

Add Security Exception

<https://60.32.129.172/demo> の Get Certificate

Confirm Security Exception

を承認すれば”Your VMKnoppix is validated.”のメッセージが出ます。



OpenPTS のコマンド詳細は下記 URL に示されています。

Command Reference of OpenPlatform Services

<http://sourceforge.jp/projects/openpts/wiki/TcdemoCommandReference>

関連論文：

- [1] Kuniyasu Suzuki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh, Trusted Boot and Platform Trust Services on 1CD Linux, IEEE International Forum on Trusted Infrastructure Technologies and 3rd Asia-Pacific Trusted Infrastructure Technologies Conference (APTC 2008)
- [2] Seiji Munetoh, Megumi Nakamura, Sachiko Yoshihama, and Michiharu Kudo, “Integrity Management Infrastructure for Trusted Computing”, IEICE TRANSACTIONS on Information and Systems, Vol. E91-D No. 5 pp. 1242-1251 (2008).

Abstract: http://search.ieice.org/bin/summary.php?id=e91-d_5_1242&category=D&year=2008&lang=E&abst=

Paper: http://search.ieice.org/bin/pdf.php?lang=E&year=2008&fname=e91-d_5_1242&abst=

5 コンパイラ関係

5.1 FailSafe-C

Fail-Safe C は、メモリ安全性を保証する ANSI C 言語のフルスペックの実装です。ANSI C 言語の仕様で定められた全てのメモリ操作（キャストや共用体を含む）に対しその安全性を保証し、全ての危険なメモリアクセスを事前に検知し防止します。

下記のようにコンパイルできます。詳細はオリジナルの HP (<https://staff.aist.go.jp/y.oiwa/FailSafeC/>)を参考にしてください。

```
$ fsc test.c -o test
$ ./test
```

5.2 VX32

ユーザレベルサンドボックスの VX32 実行環境を加えました。VX32 ではシステムコールをトラップして jail 化します。下記のようにコンパイル & 実行できます。詳細はオリジナルの HP(<http://pdos.csail.mit.edu/~baford/vm/>)を参考にしてください。

```
$ vx32-gcc test.c -o test
$ vxrun ./test
```

(注：test 単体では実行できません。)

論文：Bryan Ford and Russ Cox, “Vx32: Lightweight User-level Sandboxing on the x86”, USENIX Annual Tech 2008. pp293–306

http://www.usenix.org/events/usenix08/tech/full_papers/ford/ford.pdf

5.3 LLVM (Low Level Virtual Machine)

LLVM は独自のバイトコードを有し、プロシージャ（実行履歴）による最適化が優れているコンパイラ基盤です。実用性が高く Leopard の OpenGL スタックや iPhone のコンパイラに使われています。

下記のようにコンパイル&実行できます。詳細はオリジナルの HP(<http://llvm.org>)を参考にしてください。

```
$ llvm-gcc -emit-llvm -c test.c -o test.bc
$ lli test.bc
```

(llvm-gcc の -emit-llvm オプションで LLVM バイトコードを作成し、lli により LLVM バイトコードを実行します。)

6 全体に関する関連論文/発表

- [1] USENIX LISA 2007 (21st Large Installation System Administration conference) Dallas, USA, Nov. 14–17 “OS Circular: Internet Client for Reference”, Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, and Nguyen Anh Quynh
Paper <http://www.usenix.org/events/lisa07/tech/suzaki.html>
Slide PDF <http://openlab.ring.gr.jp/oscircular/LISA07-Slide-suzaki.pdf>
- [2] ASPLOS 08 (Thirteenth International Conference on Architectural Support for Programming Languages and Operating Systems) Poster “TPM + Internet Virtual Disk + Platform Trust Services = Internet Client”, Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Nguyen Anh Quynh, Megumi Nakamura and Seiji Muhetoh
Poster <http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-slide.pdf>
Leaflet <http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-leaflet.pdf>
- [3] USENIX Annual Tech 2008 Poster “InetBoot and VMSeed; Trusted Internet Bootloader for Hypervisor and Guest OS”, Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh
Poster <http://openlab.jp/oscircular/USENIX08Poster-suzaki.pdf>
- [4] Linux Symposium 2008, BOF “OS Circular”, Kuniyasu Suzaki
HP: http://www.linuxsymposium.org/2008/view_abstract.php?content_key=231
- [5] Virtualization Mini Summit at Ottawa Linux Symposium 2008, Virtual TPM on Xen/KVM for Trusted Computing, Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, Nguyen Anh Quynh
Slide: <http://virtminisummit.linux.hp.com/program/OLS08-Virtualization-Suzaki.pdf>
- [6] IEEE International Forum on Trusted Infrastructure Technologies and 3rd Asia–Pacific Trusted Infrastructure Technologies Conference (APTC 2008), Trusted Boot and Platform Trust Services on 1CD Linux, Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh