FreeBSD によるサーバ構築 おぼえがき

龍谷大学 理工学部　小島肇

kjm@rins.ryukoku.ac.jp

このプレゼンで説明しないこと

- **一般的なこと** (ex. kernel **の作成方法**) **については説明していません。各自で資料を参照してください。**
  - handbook (/usr/share/doc/ja/books/handbook, http://www.freebsd.org/ja/handbook/)
  - FAQ (/usr/share/doc/ja/books/faq/, http://www.freebsd.org/ja/FAQ/)
  - http://www.freebsd.org/ja/
  - http://www.jp.freebsd.org/

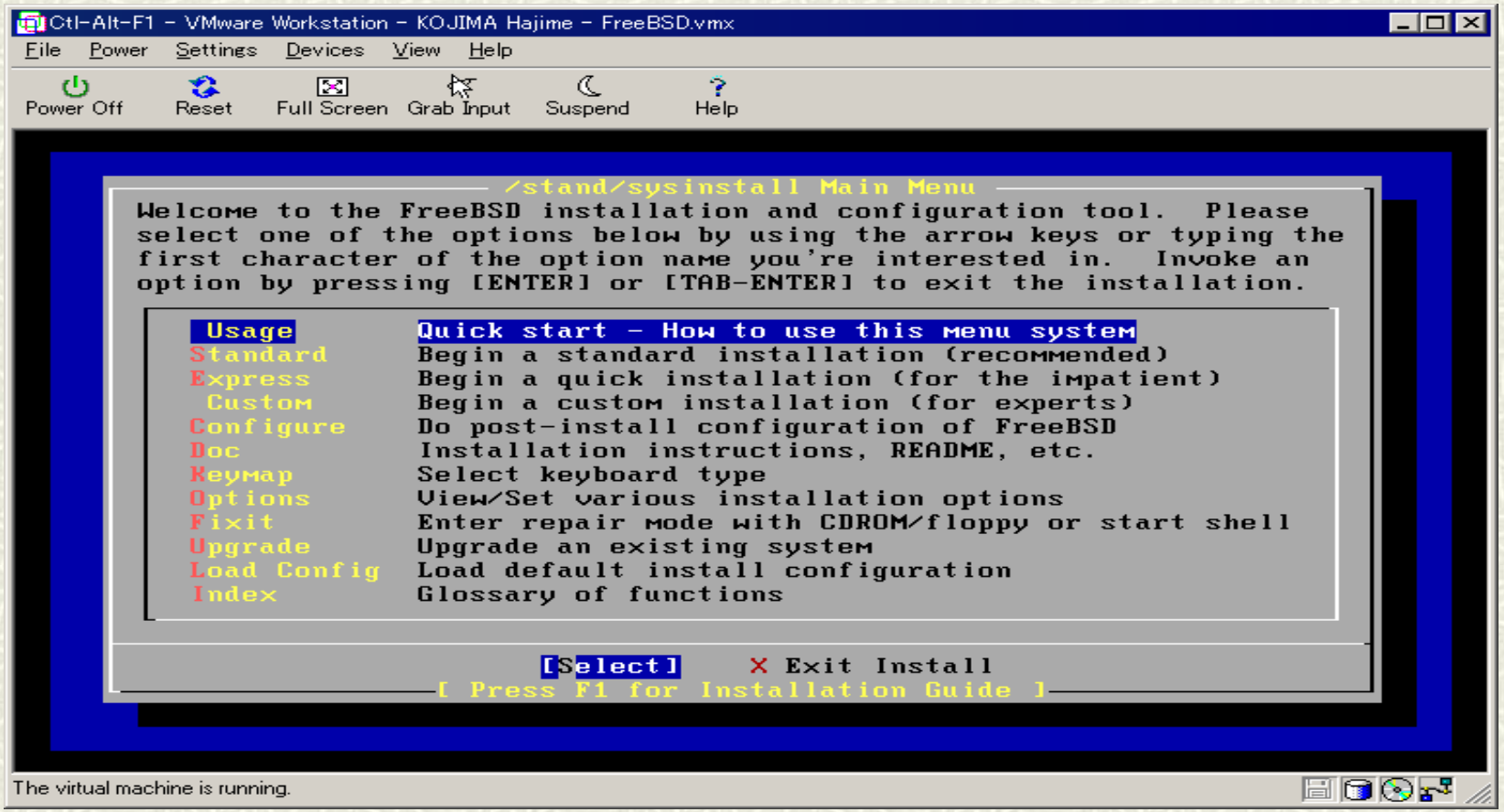
Why FreeBSD?

- FreeBSD is free.
- **安定して動作する**
- **利用者が多い → 情報が多い**
  - S/N **比も高い**
- **セキュリティもがんばっている**
  - ports **のセキュリティ勧告を出しているのは** *BSD **中** FreeBSD **だけ**
  - OS **の** binary patch **の配布も開始**
- **全体が単一の** OS **である安定感**
  - **モジュール構造の** Linux **にも便利な点はある…**

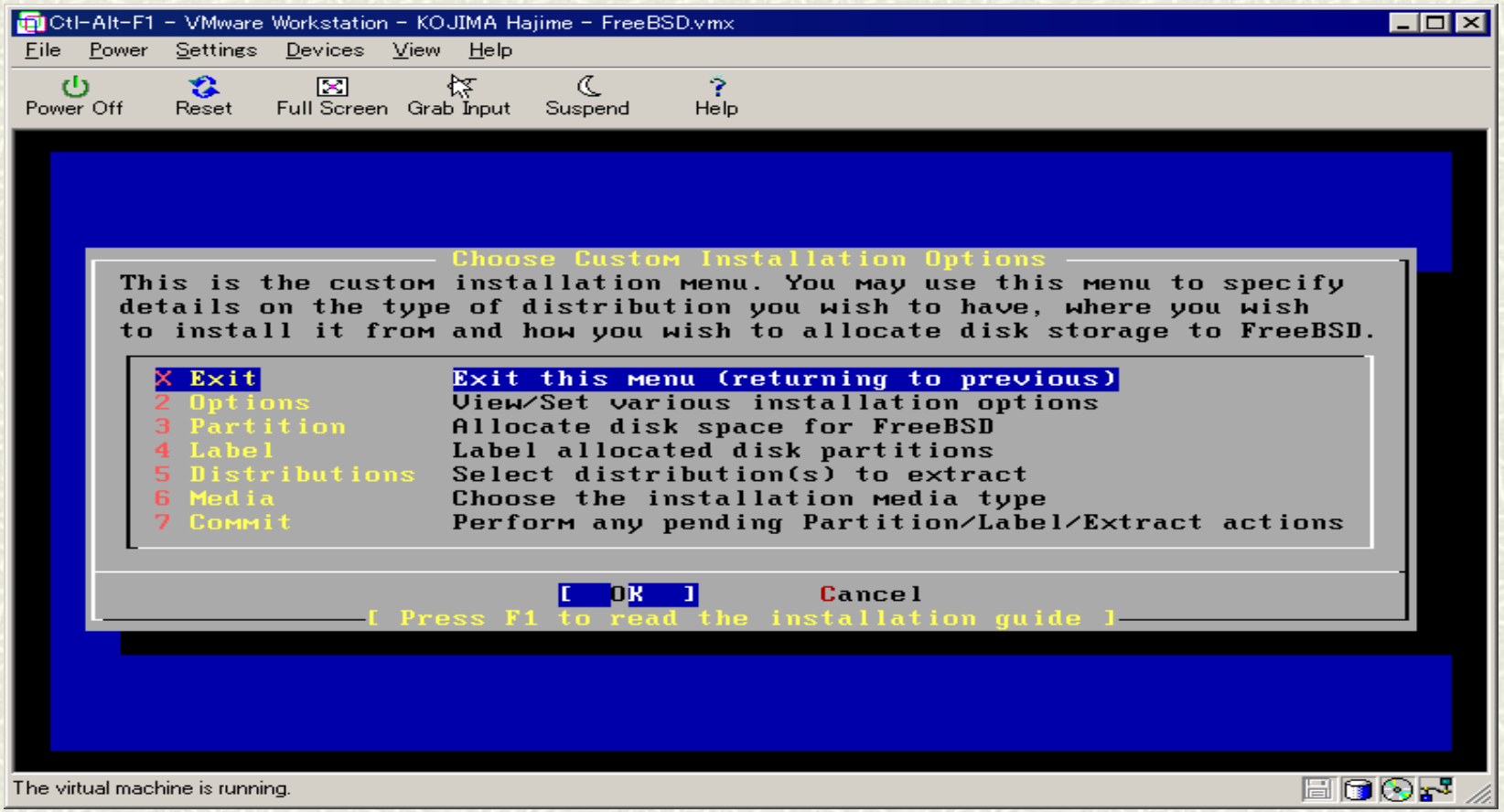
インストール

- ふつう、最新リリース版ですよね
  - ようやく 4.4-RELEASE が出たようです
  - -stable も、たま〜にアレゲなことがあるようです
  - 4.3-RELEASE から、「RELENG_4_3」という「最低限の fix」のためのブランチがつくられるようになった
    - 当然 RELENG_4_4 もつくられている

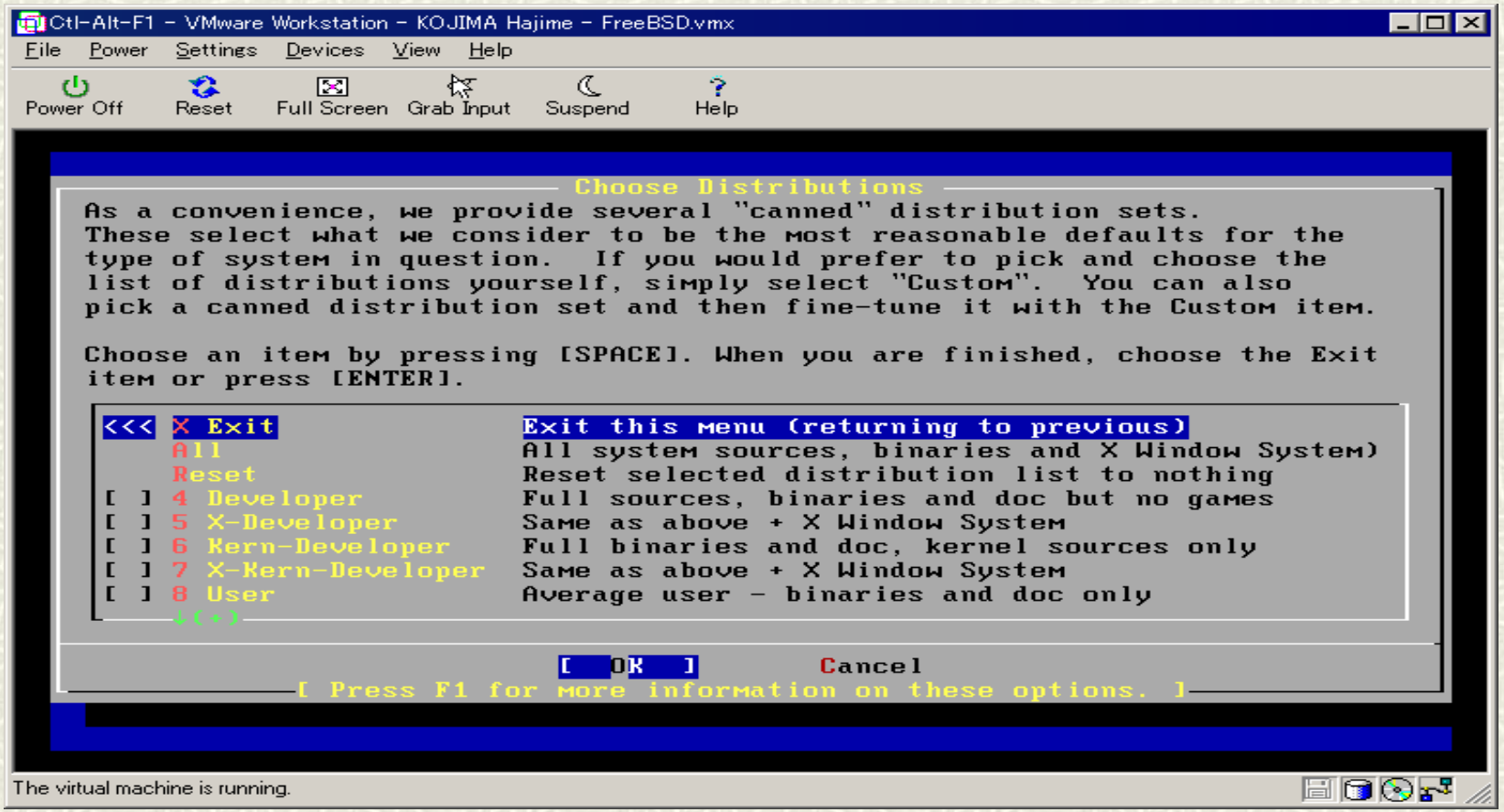
インストール


Ctl-Alt-F1 - VMware Workstation - KOJIMA Hajime - FreeBSD.vmx
File Power Settings Devices View Help
Power Off Reset Full Screen Grab Input Suspend Help
/stand/sysinstall Main Menu
Welcome to the FreeBSD installation and configuration tool. Please select one of the options below by using the arrow keys or typing the first character of the option name you're interested in. Invoke an option by pressing [ENTER] or [TAB-ENTER] to exit the installation.
Usage Quick start - How to use this menu system
Standard Begin a standard installation (recommended)
Express Begin a quick installation (for the impatient)
Custom Begin a custom installation (for experts)
Configure Do post-install configuration of FreeBSD
Doc Installation instructions, README, etc.
Keymap Select keyboard type
Options View/Set various installation options
Fixit Enter repair mode with CDROM/floppy or start shell
Upgrade Upgrade an existing system
Load Config Load default install configuration
Index Glossary of functions
[Select] X Exit Install
[Press F1 for Installation Guide]
The virtual machine is running.

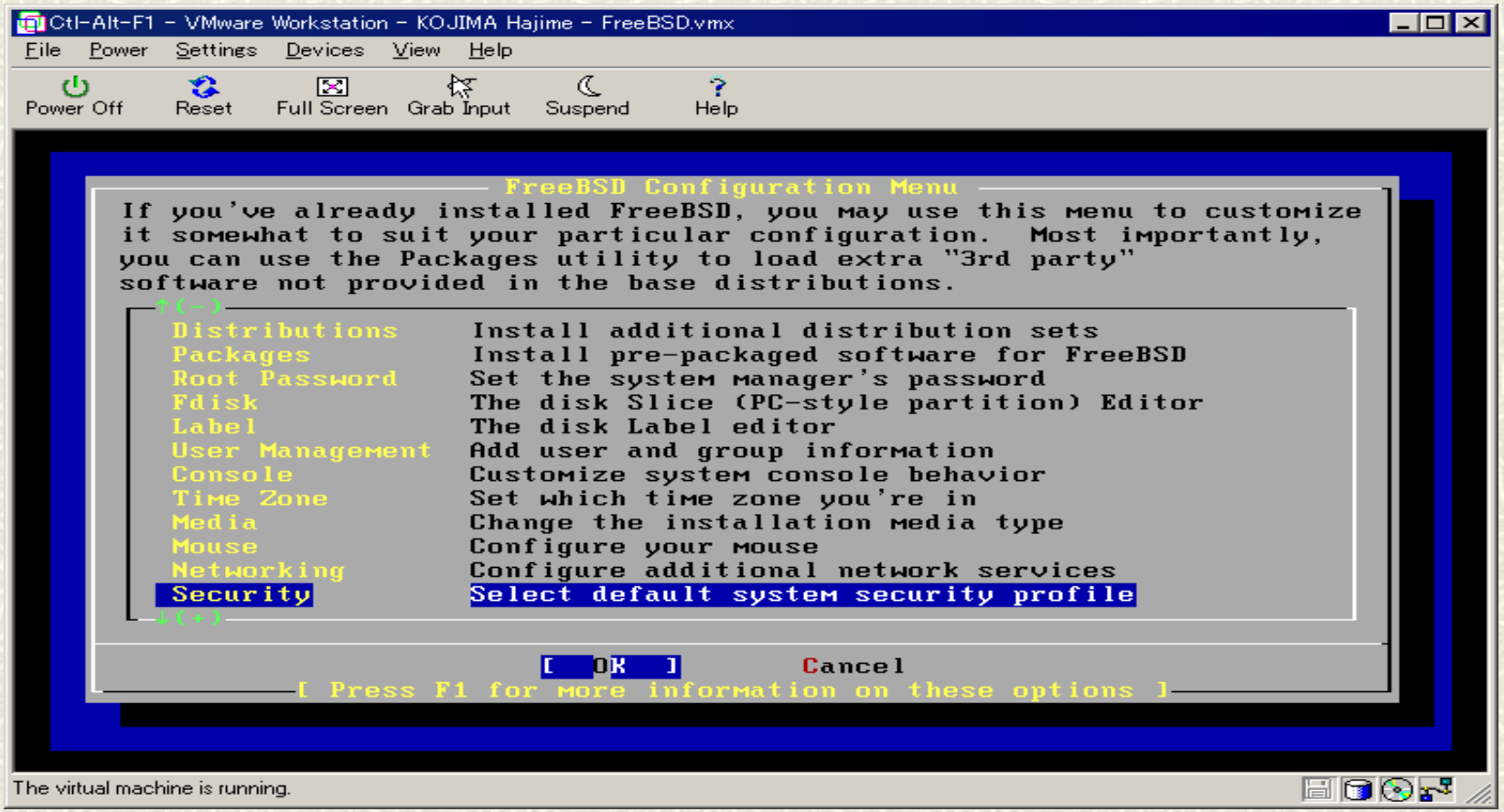
Custom Installation



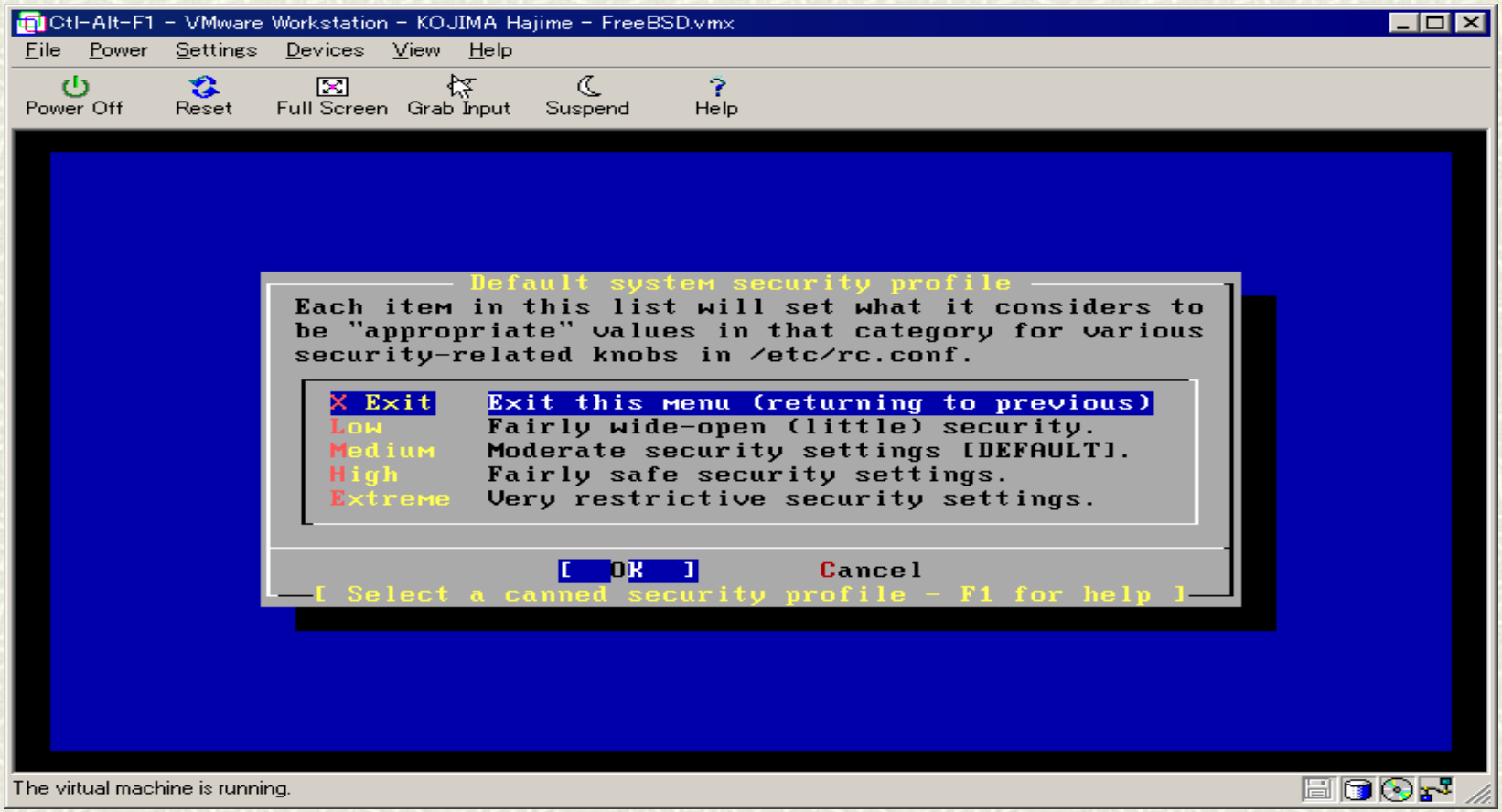
Distribution



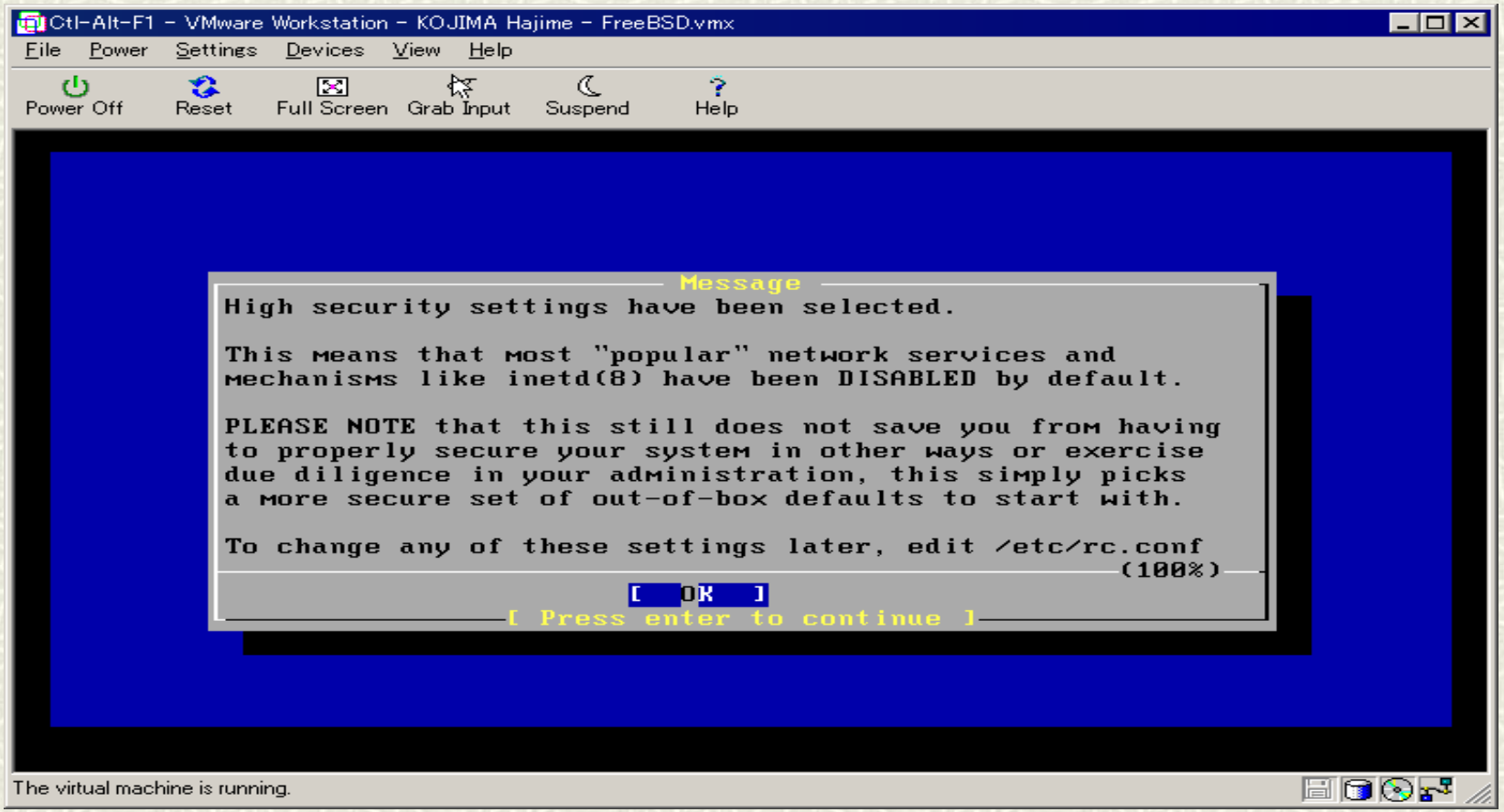
FreeBSD Configuration Menu



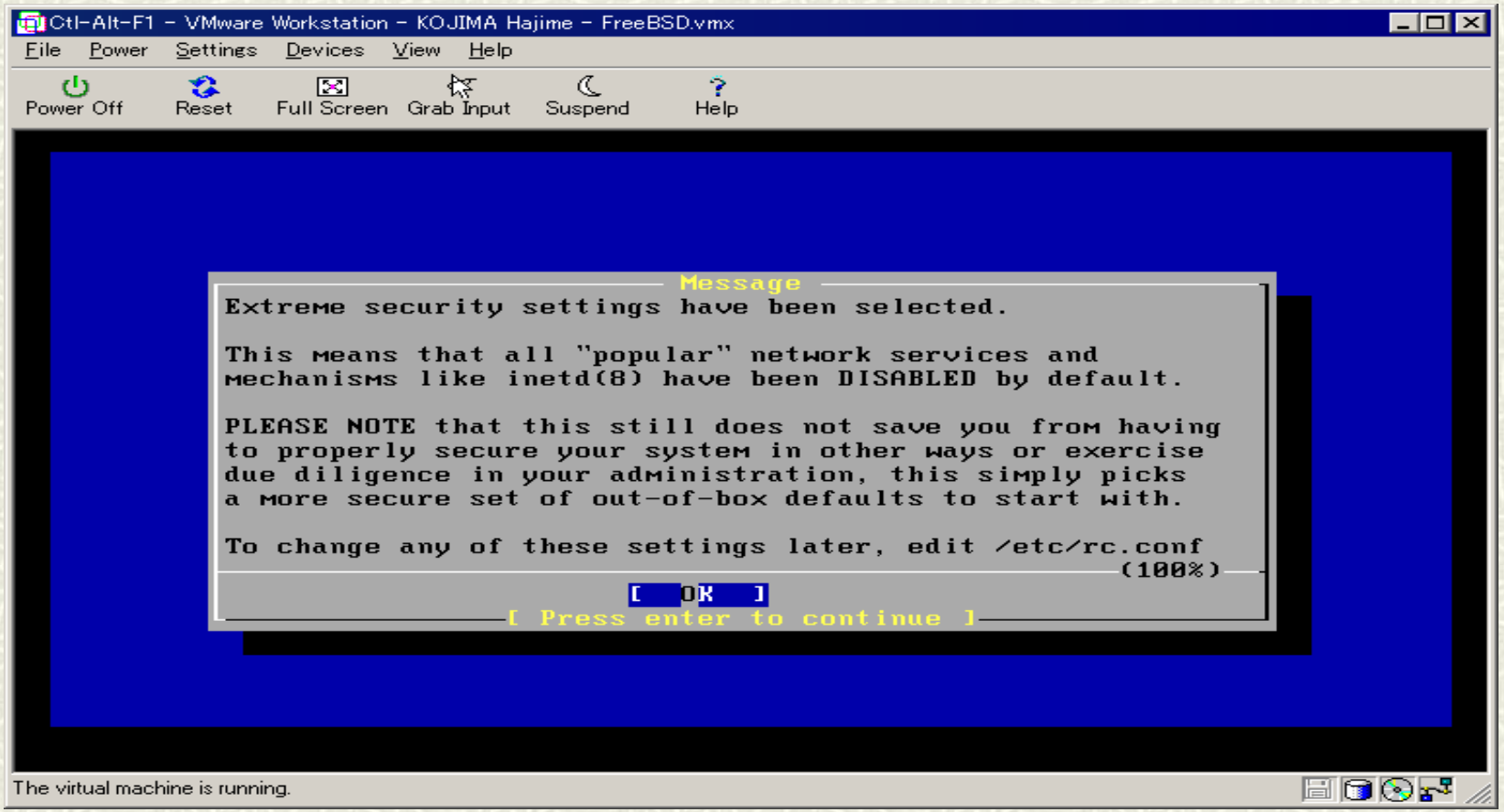
Default system security profile



system security = high



system security = extreme



再起動

- うまく boot しなかったら….
  - 悩んでください :-)

セキュリティパッチの適用

- 既存のセキュリティパッチを適用しておく。
  - http://www.freebsd.org/ja/security/
  - http://www.freebsd.org/releases/4.4R/errata.html
- コマンド、ライブラリなどについては即時に
  make all; make install
- kernel patch については、patch 適用後に
  kernel の調整を行う過程で調整

kernel の調整

- kernel config の基本:
  http://www.freebsd.org/ja/handbook/kernelconfig.html
- 個人的にやってること:
  - maxusers は増やす (最低 128)
    - 4.4-RELEASE では動的に制御できるようです
  - bpf は外す
    - nmap とか snort とか iplog とかを使う場合は bpf がないと困るんだけど…

kernel の調整 (cont.)

- options:
  - SC_DISABLE_REBOOT
    syscons コンソールドライバでの CTRL-ALT-DEL リブートを禁止
  - IPFILTER, IPFILTER_LOG
    ip-filter を使っているので
  - TCP_DROP_SYNFIN
    SYN+FIN なパケットは落とす (web server には推奨されないようです)
  - TCP_RESTRICT_RST
    RST がいっぱい来たら落とす (DoS 対策)
  - ICMP_BANDLIM
    ICMP 帯域制限 (DoS 対策)
- 詳細は /usr/src/sys/i386/conf/LINT を

kernel の調整 (cont.)

- /etc/sysctl.conf (例)

```
kern.ipc.somaxconn=1024
kern.ipc.maxsockets=16384
kern.ipc.nmbclusters=65536
kern.maxfiles=32768
kern.maxfilesperproc=16424
```

- /boot/loader.conf (例)

```
hw.ata.wc=1
hw.ata.tags=1
```

  - 4.4-RELEASE では hw.ata.wc=1 はデフォルトで有効のようです

kernel の調整 (cont.)

- /etc/rc.conf

```
tcp_restrict_rst="YES"
tcp_drop_synfin="NO"
```

kernel の調整 (cont.)

- kernel securelevel

-1	なんでもあり (default)
0	single user 時は –1 と同じ。multi user 時に 1 と同じ。
1	mount しているファイルシステムの raw デバイス、/dev/mem, /dev/kmem には write アクセスできない。kernel module は load できない。変更不可フラグ、追加のみフラグ (ls –lo で確認できる) を無効にできない。
2	mount していない raw デバイスも write アクセスできない。unmount できない。時間の変更は 1 秒以内。
3	IP フィルタルール、dummynet 設定を変更できない。

kernel の調整 (cont.)

- kernel securelevel (cont.)
  - 例:
    kern_securelevel_enable="YES"
    kern_securelevel="1"
  - たとえば kern_securelevel="1" の場合に kernel の upgrade をしようとすると…
    - 一旦 kernel_securelevel="-1" で reboot
    - kernel インストール
    - 再度 kernel_securelevel=1 で reboot
    - file integrity checker 情報を更新?
  - kernel securelevel はリブートしないと下げられない

userland の調整

- /etc/inetd.conf
  - ftpd には –l をつける (`-l -l`)
  - telnetd には –h –U をつける
  - 他は止める
  - /etc/rc.conf で inetd_flags="-wWl" する
- One-Time Password
  - telnetd や ftpd を使うならぜひ…
  - S/Key と OPIE が使える
    - 安定度 – S/Key, RFC 準拠 – OPIE
    - FreeBSD の「標準」は S/Key
    - 私は S/Key の出力を RFC ライクに変更して使っている

userland の調整 (cont.)

- /etc/rc.conf
  - 各種 daemon の起動制御
  - /etc/default/rc.conf を見ながら…
- /etc/login.conf
  - `:minpasswordlen=8:` を追加
- /etc/syslog.conf, /etc/newsyslog.conf
  - 好みに応じて…
  - 私は、デフォルトよりは長めに記録するよう newsyslog.conf を変更している

TCP/IP フィルタリング

- ipfw
  - FreeBSD 標準
    - MacOS X でも使える
  - dummynet(4) を利用した帯域制御
  - netgraph(4) を利用した細かい制御 (?)
    - すんません、よく知りません…
  - /etc/rc.firewall にわかりやすい実例あり。設定例:

```
firewall_enable="YES"
firewall_type="client"
```

TCP/IP フィルタリング (cont.)

- ip-filter
  - 多くの UNIX で使える
    - *BSD, Linux, Solaris, HP-UX, AIX, …
  - 広く利用されている
  - ライセンスがアレゲ
    - 独自に patch あてたものを配布できない、とか…
    - OpenBSD は ip-filter を捨て、pf (packet filter) へ
  - /etc/rc.conf 記述例:

```
ipfilter_enable="YES"
ipfilter_program="/sbin/ipf -Fa –f"
ipfilter_rules="/etc/ipf.rules"
```

TCP/IP フィルタリング (cont.)

- 機能的には、ipfw は ip-filter に劣らない
  - むしろ、今では優れている?

tcp_wrapper による接続制限

- /etc/hosts.allow で定義
  - たいていの Linux distrib. と違い、PROCESS_OPTIONS が有効になった tcp_wrapper がインストールされているので注意。/etc/hosts.deny は使わない。hosts_options(5) 参照。
  - inetd, sendmail, portmap, ssh に tcp_wrapper が組み込まれている。
  - OS をアップグレードすると、/etc/hosts.allow は常に初期状態 (サンプルファイル) になってしまうようだ。必要なら /usr/tmp/etc/hosts.allow から戻すなりしよう。

その他の接続制限

- かな漢字変換サーバ Canna - /etc/hosts.canna
  - 接続を許可するホスト名を記述
  - localhost からの接続のみを許可するなら:

    ```
    localhost
    unix
    ```

    unix は UNIX ドメインソケット。
- ラインプリンタデーモン lpd - /etc/hosts.lpd
  - 接続を許可するホスト名を記述
- TCP/IP パケットフィルタも設定した上で、上記も設定することが望ましい。

設定のヒント

- /etc/ipf.rules の原型
  - /usr/src/contrib/ipfilter/mkfilters
- ingress/egress filter rule
  http://www.sans.org/dosstep/index.htm
  - /etc/rc.firewall の simple で定義されている (ipfw)
  - /usr/src/contrib/ipfilter/IPF.KANJI が参考になる (ip-filter)
- default allow? default deny?
  - 状況に応じて…

/usr/ports/security/ みてある記

- メールサーバ用 anti-virus ソフト
  - amavis-perl
  - inflex
  - drweb-sendmail (drweb.ru)
  - qmail-scanner (qmail 用、ports にはない)
- 脆弱性スキャナ
  - arirang (web server)
  - nessus (全般)
  - saint (全般)
  - nmap (port scanner)

みてある記 (cont.)

- IDS
  - aafid
  - snort
  - portsentry – portscan detector
- file integrity checker
  - aide
  - integrit
  - tripwire (**古いやつ**…1.x **用**)
    - 2.3.1-2 port
  - chkrootkit

みてある記 (cont.)

- password cracker/checker
  - john
  - crack
  - l0phtcrack
  - cracklib
  - checkpassword
- log checker
  - logcheck
  - swatch

みてある記 (cont.)

- **暗号化**
  - openssh
  - openssh-portable
  - lsh (GNU ssh)
  - zebedee
  - cfs – cryptographic file system
- danger tools
  - dsniff
- others
  - ca-roots

…and now, network is battlefield.

- for more info:
  - http://www.jp.freebsd.org/
  - http://www.st.ryukoku.ac.jp/~kjm/security/memo/