HP-UX 11iv2 入門
～セキュリティ強化＆設定方法解説～

コンサルティング・インテグレーション統括本部
IT コンサルティング本部
テクノロジーコンサルティング部

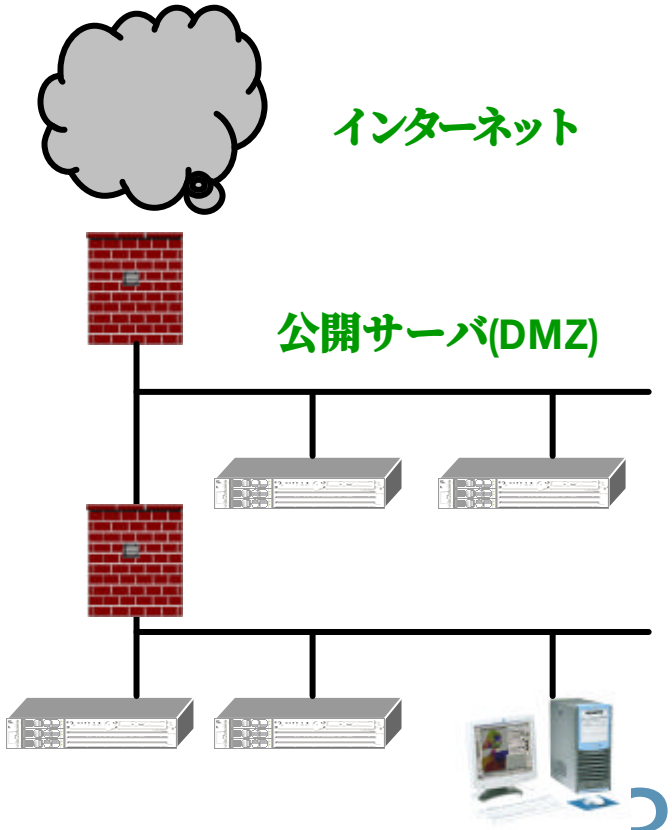
Agenda

- HP-UX11i v2 セキュリティ
- Install Time Security
- Bastille
- 参考情報（URL）

コンピュータシステムにおけるセキュリティ

- コンピュータシステムにおけるセキュリティは社会問題
  - インターネットの普及
  - 多様なサービスの提供

- セキュリティを強化するには・・・・
  - 環境　設置場所、ネットワーク接続)
  - オペレーティング・システム
  - アプリケーション
  - システム運用



オペレーティングシステムセキュリティ(1)

- 識別と認証 — ユーザ名・IDで識別、パスワードで認証
  - シャドウパスワード、Kerberos, LDAP, PAM、ログイン制御
- 認可 — root ユーザは、すべての権限を持つ
  - 制限つき(Restricted)SAM、SCM
- アクセス制御 — ファイルパーミッションによる制御
  - ACL(Access Control List)による任意のユーザ・グループ
- 監査 / アカウンタビリティー システムイベントの記録
  - syslog, sulog, wtmp、システムコール監査
- オブジェクトの再利用 — 以前のデータの消去、初期化
  - メモリバッファの初期化

オペレーティングシステムセキュリティ(2)

- 侵入阻止 ― 侵入を阻止するような設計・実装
  - スタック実行保護機能
- 侵入検知 ― システムを監視し、セキュリティ問題を検知
  - Host IDS(Intrusion Detection System)
- システムの強化 ― 不要なサービスの停止
  - Bastille, Security Patch Check, IPFilter
- 保証 ― 提供されているセキュリティ機能は本当に安全？
  - 品質、信頼性、標準適合の各要件に関する社内基準をクリア
  - CERT, FIRST等のコンピュータセキュリティセンターからのセキュリティ報告の検討、必要に応じた対応
  - セキュリティ標準への準拠
    - CCITSE EAL4-CAPP 認証(HP-UX 11.11)

システムの堅牢化

システムのセキュリティを強化するには、
最小特権、最小限のサービス提供

- 最小特権
  それぞれのアプリケーションあるいはOSの
  コンポーネントは必要とするユーザにのみ権限を与える
- 最小限
  脆弱性をもっている可能性のあるサービスだけでなく、
  必要でないサービスはすべて停止

↓

OSで提供されているサービス、システムごとに設定する必要性

↓

セキュリティ強化/ロックダウンツール ***Bastille***
OSインストール時のセキュリティ設定 ***Install Time Security***
の提供

HP-UX 11iv2 Install Time Security

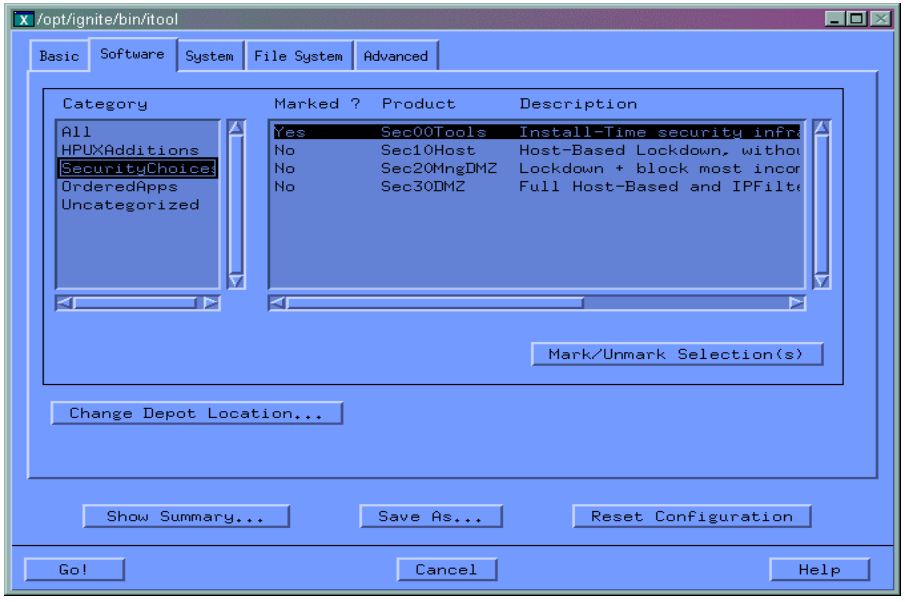
- HP-UX OE に含まれます
- HP-UX インストール/アップデート時のセキュリティ設定
  - 一貫性ある設定
  - 環境に応じたセキュリティ強化
  - インストールと同時に堅牢なシステム構成が可能
    - Bastille による設定変更も可

4つのセキュリティレベルが選択可:

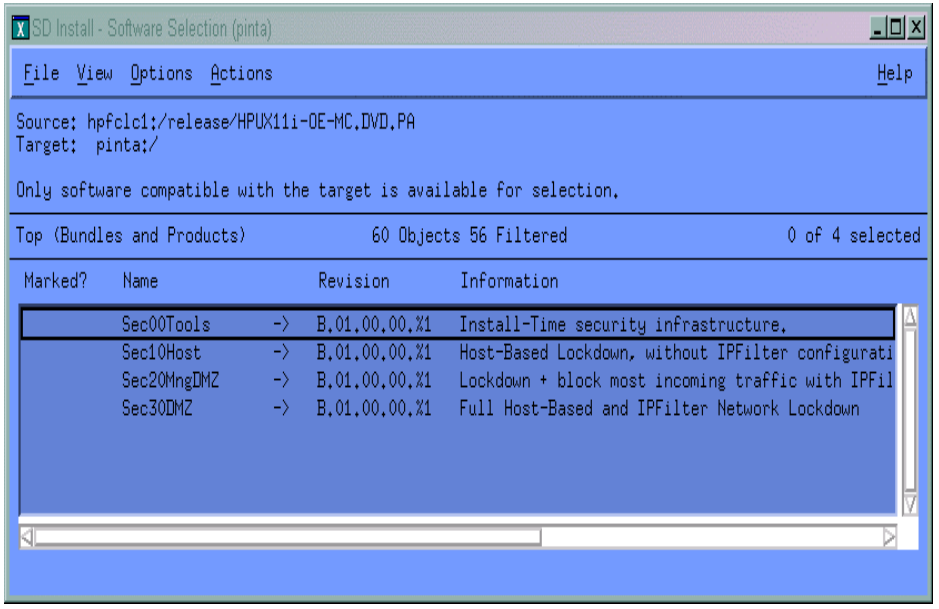
1. Tools only（Sec00Tools）– Bastille、SSH、Security Patch Check および IPFilterのインストールのみ
2. Host（Sec10Host）– 約50のhostベースのロックダウンを行う
3. Managed DMZ（Sec20MngDMZ）– いくつかのセキュアなプロトコルのみを接続
4. DMZ（Sec30DMZ）– SSH以外のコネクション をブロックします

Install-Time Security の設定方法

1) Ignite / UX



2) Software Distributor



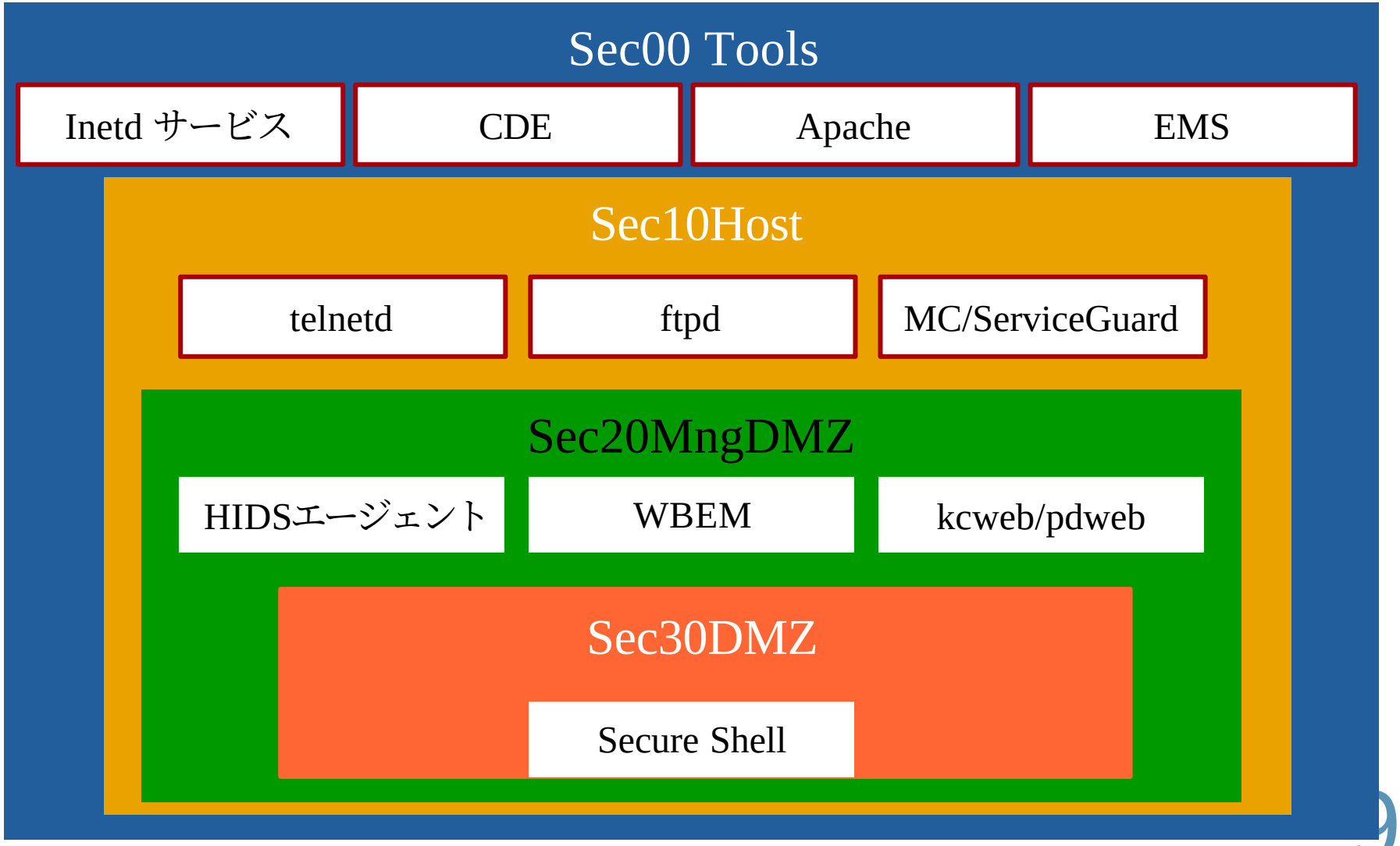
3) Manual

```
# swinstall –s <depot> -x autoreboot=true <level>
```

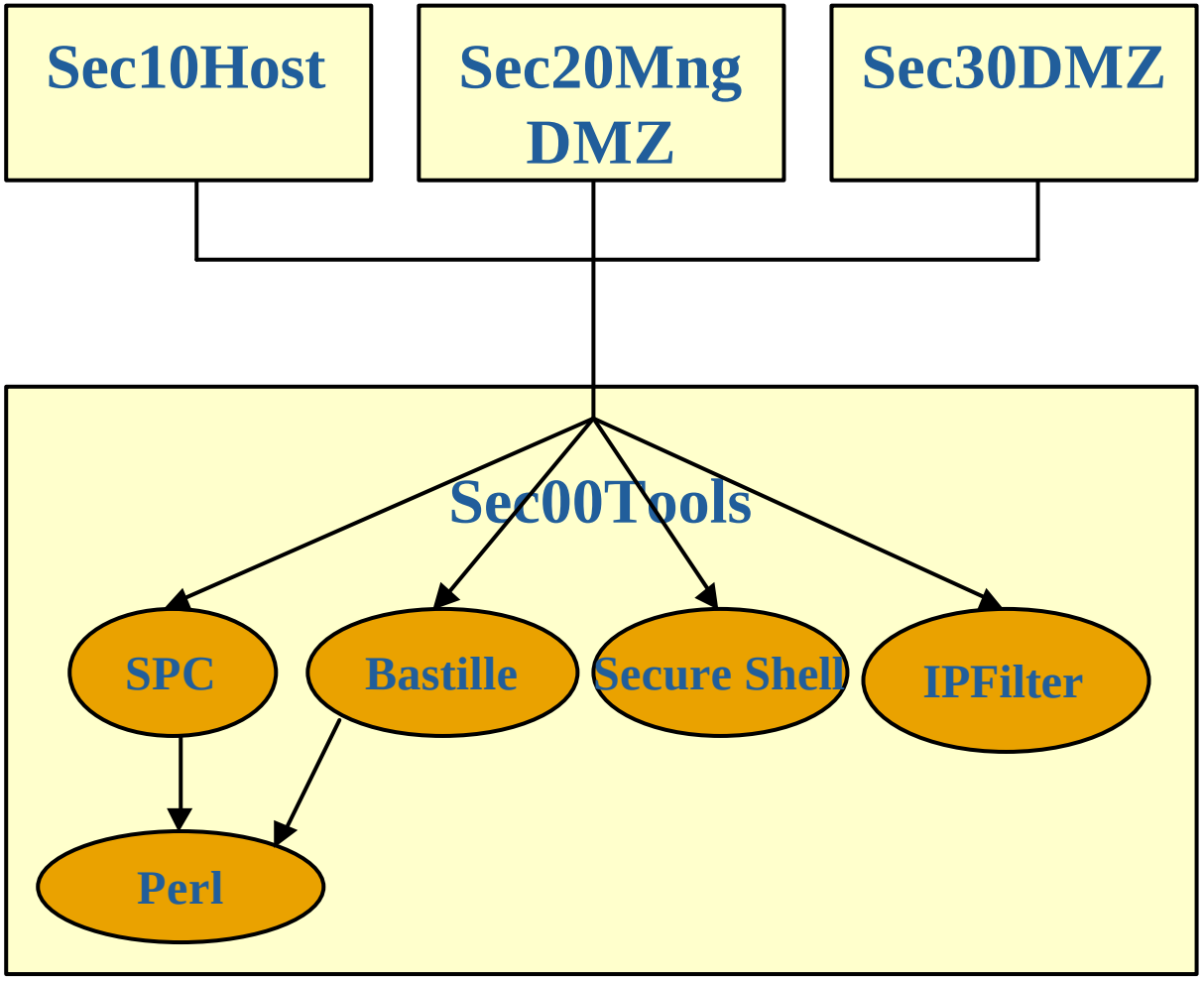
4) Update / UX

```
# update-ux –s <depot> <OE> <level>
```

セキュリティ構成バンドルと主なアプリケーション



セキュリティ構成バンドルの関係



ホスト要塞化ツール Bastille

- Perlベースのセキュリティ強化/ロックダウン ツール
- 対話式に設問に答えるだけで、カスタムなセキュリティ設定が可能
- Linuxシステム上で使用するためにオープンソースコミュニティで開発

  http://bastille-linux.org
- HP-UX の他にも
  - Red Hat Linux
  - TurboLinux
  - Mac OS X　など

Bastille の機能

- sendmailなどのシステムdaemonの設定を変更し、セキュリティ強化を行います
- echoや fingerなどの不必要なサービスを停止します
- chrootによる “jails”構成を行います
  - webや Domain Name Service (DNS)などのInternetサービスにたいして、追加のセキュリティ層を構築します
- 管理者にアドバイスを与えるインターフェース
- Bastilleの設定を以前の状態に戻せる revert機能
- シャドウパスワード Trustシステム /tcb、業界標準 /etc/shadow)の切換え
- Security Patch Checkツールの自動実行設定
- IPFilter firewallの設定

HP-UX 11iv2 でのBastille の起動

- Install Time Security
  - ログファイル：
    level-application-actions
  - エラーログファイル：
    level-application-errors

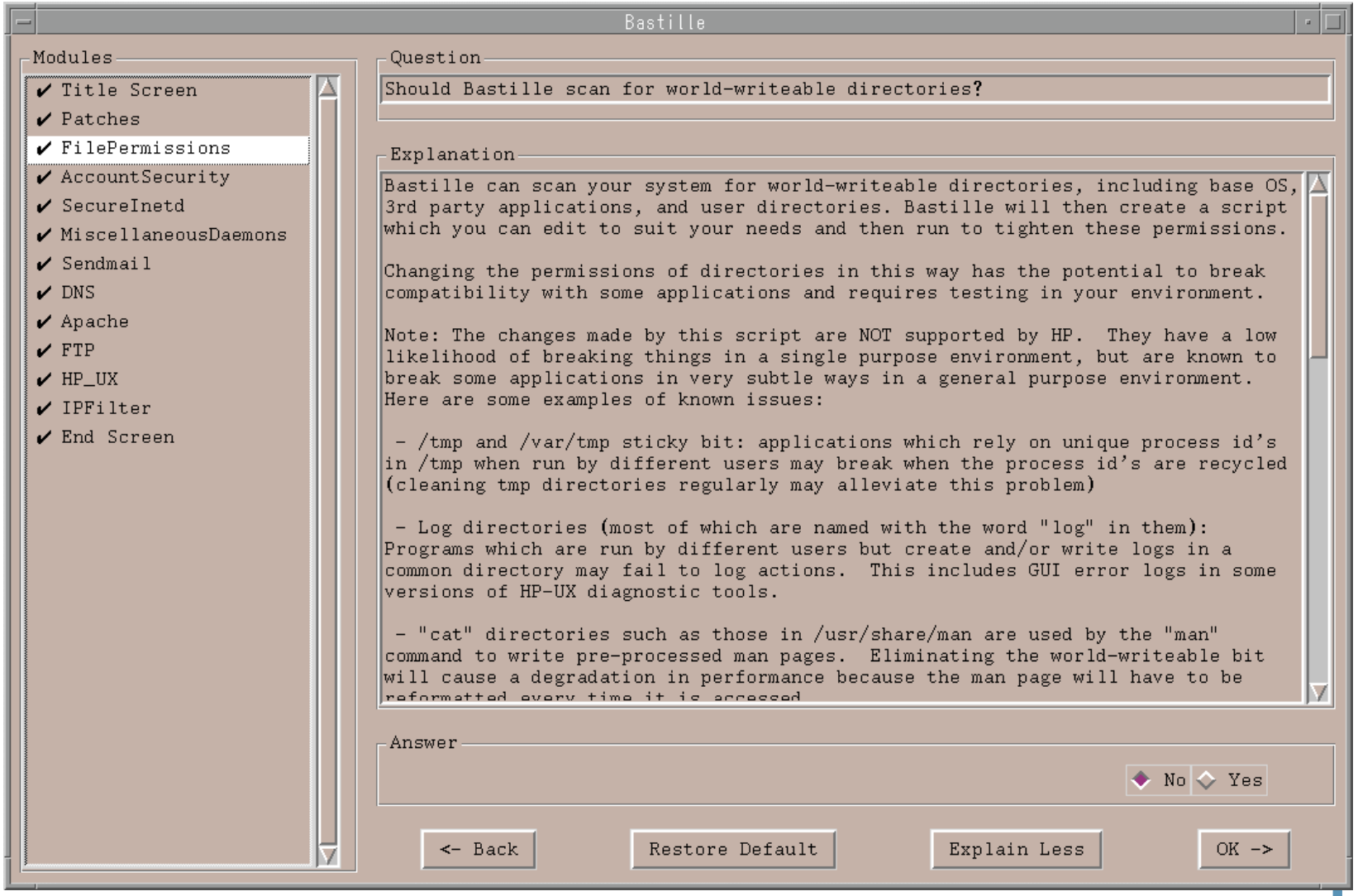
- 対話型セッションの起動
  # bastille
  (X-Window displayが必要)

- 構成ファイルから、
  システムに変更反映
  # bastille -b

Bastille 実行時の出力

```
NOTE:    Entering Critical Code Execution.
         Bastille has disabled keyboard interrupts.

NOTE:    Bastille is scanning the system configuration...

Bastille is now locking down your system in accordance with your
answers in the "config" file.  Please be patient as some modules
may take a number of minutes, depending on the speed of your
machine.

Executing File Permissions Specific Configuration
Executing Account Security Specific Configuration
Executing Inetd Specific Configuration
Executing Daemon Specific Configuration
Executing Sendmail Specific Configuration
Executing DNS Specific Configuration
Executing Apache Specific Configuration
Executing FTP Specific Configuration
Executing HP-UX's Security Patch Check Configuration
Executing IPFilter Configuration
Executing HP-UX Specific Configuration

Please check
/var/opt/sec_mgmt/bastille/TODO.txt
for further instructions on how to secure your system.
```

Bastille 起動画面



HP-UX Bastille's Modules

- Patches
  - 迅速なセキュリティパッチ対応
- File Permissions
  - 脆弱性の排除
- Account Security
  - アクセス制御
- Secure Inetd
- Miscellaneous Daemons
  - 不要なサービスを起動しない
- Sendmail
- DNS
- Apache
- FTP
  - 不要なサービスを起動しない
  - 安全な運用
- HP-UX
  - HP-UX 固有のシステム強化
- IPFilter
  - ファイアウォール

HP-UX Bastille's Patches and File Permissions Modules

- SPC(Security Patch Check) 設定
  - SPC のダウンロード・インストール手順の提示
  - SPC の自動実行
    - SPC 実行時間は指定可能
    - カタログファイルのダウンロード時のプロキシ設定
- File Permissions 設定
  - World-Writeable ディレクトリ・スキャン
    - 編集可能なパーミッション変更スクリプトを自動作成
    - swverify でのエラーを防ぐためにSD ファイルのチェック

```
# drwxrwxrwx   bin   bin   Feb   19   2003   /opt/netscape/plugins
/usr/bin/chmod 1777 "/opt/netscape/plugins" ; ¥
/usr/sbin/swmodify -x files="/opt/netscape/plugins" NS-communicate.NETSCAPE-RUN
echo "/usr/bin/chmod 0777 ¥"/opt/netscape/plugins¥" ; /usr/sbin/swmodify ¥
 -x files=¥"/opt/netscape/plugins¥" NS-communicate.NETSCAPE-RUN" >> $REVERTPERMS
```

hp-ux11i セキュリティパッチ・チェックツール (Security Patch Check)

- 利用中のhp-ux11i システムにインストールされているファイルセットやパッチを分析し報告
- そのシステムに適用を推奨するセキュリティ関連パッチをレポート
- システム上にインストールされているパッチのリコールを警告

```
*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.23) from kios
Security catalog: /etc/opt/sec_mgmt/bastille/security_catalog
Security catalog created on: Sun Feb  8 11:14:40 2004
Time of analysis: Mon Feb  9 19:03:07 2004

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
1  PHNE_29913     281     No     No       No      sendmail(1m) 8.11.1
2  PHSS_29966     299     Yes    No       No      HP DCE 1.9 client cumulative
3  PHSS_30013     297     No     No       No      CDE Base
-------------------------------------------------------------------------------
*** END OF REPORT ***
NOTE:    Security bulletins can be found ordered by number at
         http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
```

HP-UX Bastille's Account Security Module

- デフォルトシステム"umask"
  - bash, csh, ksh, zsh のデフォルト設定
    - /etc/profile, /.profile, /etc/csh.login
  - "/etc/default/security" システム umask
    - HP-UX 11.22 以降で設定可能
- シャドウ・パスワード(/etc/shadow)
- シングルユーザモードでのパスワード保護
  - "/etc/default/security" BOOT_AUTH
- セキュリティ監査

HP-UX の 2つのモード

- 標準モード(Standard Mode)
  - デフォルト
    オペレーティングシステム機能
  - 通常の運用で使用
  - リリースごとに
    セキュリティ機能を強化
- 高信頼性モード
  (Trusted Mode)
  - C2セキュリティ準拠
  - セキュリティ機能の強化
  - 簡単なモード切替え
    (SAM, コマンド)
    - HP-UX コア機能として実装

高信頼性モード (高信頼システム)

- システム監査
  - 各ユーザが実行したすべての システム・コールの トレースが 可能
- パスワード強化
  - アカウントの無効化
  - 80文字までのパスワード長
  - ランダム・パスワード・ジェネレータ
- ログイン制限
  - 時間
  - デバイス

HP-UX Bastille's Account Security Module

- ユーザパスワードポリシー
  - パスワード履歴
  - パスワード変更間隔最大日数
  - パスワード変更間隔最小日数
  - パスワード期限切れ報告

- ファイル

  /etc/default/security
  (標準モード)

  /tcb/files/auth/system
  (高信頼性モード)

HP-UX Bastille's Account Security Module

- ログインポリシーの設定
  - ホームディレクトリが存在しないユーザのログインの拒否
    - /etc/default/security ABORT_LOGINON_MISSING_HOMEDIR=1
  - "/etc/nologin" 機能の有効化
    - /etc/default/security NOLOGIN=1
  - ユーザあたりに許可されるログイン数
  - "su" コマンド実行時のデフォルトPATH 環境変数
    - /etc/default/security SU_DEFAULT_PATH
  - ネットワーク tty からのルートログイン制限
    - /etc/securetty ファイル作成

HP-UX Bastille's Secure Inetd Module

- Inetd service audit
  - telnet サービス
    - クリアテキストリモートログインデーモン
  - ftp サービス
    - クリアテキストリモートファイル転送デーモン
  - login, shell, exec サービス
    - rlogind, remshd, rexecd を起動
  - TFTP サービス
    - Trivial File Transfer Protocol (TFTP) は、UDP ベースのファイル転送プロトコル

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - bootp サービス
    - Dynamic Host Configuration Protocol (DHCP) サーバ
    - Internet Boot Protocol (BOOTP) サーバ
    - DHCP/BOOTP リレー・エージェント
  - finger サービス
    - RFC 742 Name/Finger プロトコル
  - uucp サービス
    - UUCP (Unix to Unix copy) は、UNIXシステム間でファイルのコピーを行う
  - ntalk サービス
    - リモートユーザー通信サーバ

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - ident サービス
    - TCP/IP の標準 IDENT ユーザ識別プロトコルを実装
  - daytime, discard, chargen, and echo サービス
    - daytime: 現在の日時を人間が読める文字列として送信 (RFC 867)
    - discard: /dev/null と同様に、受信したすべてのデータを破棄 (RFC 863)
    - chargen: Character Generator は、特に定義されていないデータストリームを送出。(RFC 862)
    - echo: 単純に受信したパケットを返す (RFC 862)

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - time サービス
    - inetd に内蔵されているサービスで、1900年1月1日午前0時からの時間を、マシンが読み取れる秒単位の形式で生成。
  - klogin および kshell サービス
    - これらのサービスは、Kerberos 認証で使用。
  - dtspcd, cmsd, ttdbserver
    - dtspcd: 他のシステムでプロセスを実行するために使用される Desktop Sub process Control サービス
    - cmsd: ネットワーク経由で Sun の Calendar Manager ソフトウェアデータベースを実行するために使用
    - ttdbserver: Sun の ToolTalk Database Server は、OpenWindows プログラム間の相互通信を可能にする

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - recserv サービス
    - HP SharedX Receiver Service は、明示的に xhost コマンドを一切実行することなく、Xウィンドウが稼動しているほかのマシンから共用ウィンドウを取得する場合に使用
  - swat サービス
    - Samba の設定ユーティリティ
  - printer サービス
    - リモートスプールの要求を受け付けるラインプリンタデーモン
- Inetd ロギング指定
- "Authorized Use Only" メッセージ
  - 侵入者への警告
    - /etc/issue, /etc/motd
    - /etc/inetd.confのtelnet, login, kloginに -b, -B /etc/issue を追加

HP-UX Bastille's Miscellaneous Daemons Module

- NFS サーバデーモンの非アクティブ化
- NFS クライアントデーモンの非アクティブ化
  - Autofs
  - ブロックI/O デーモン(biod)
- NIS サーバデーモンの非アクティブ化
- NIS クライアントデーモンの非アクティブ化

非アクティブ化（NFSサーバデーモン)

- /sbin/init.d/nfs.server stop を実行
- /etc/rc.config.d/nfsconf の NFS_SERVER=0 に設定

HP-UX Bastille's Miscellaneous Daemons Module

- SNMPDの非アクティブ化
- ptydaemon、vtdaemon の非アクティブ化
  - ptydaemon シェル階層マネージャ (shl) ソフトウェアで使用
  - "vtdaemon" は、リモートログイン機能を "ptydaemon" を使用して提供
- "pwgrd" の非アクティブ化
  - パスワードおよびグループのハッシュとキャッシュを管理するデーモン
- "rbootd" の非アクティブ化
  - HP 独自のブート/ ファイル転送プロトコル(Remote Maintenance Protocol)
- リモートのXログインの拒否
  - X サーバとのリモート接続を行うプロトコル

HP-UX Bastille's Sendmail Module

- sendmail デーモンの非アクティブ化
- メールキューを処理するために定期的に sendmail を起動
- SMTP (Simple Mail Transport Protocol) VRFY および EXPN コマンドの無効
  - VRFY コマンド
    - 受信者の存在確認
  - EXPN コマンド
    - 受信者のエイリアス/一覧内容の拡張

HP-UX Bastille's DNS Module

- BIND (Berkeley Internet Name Domain) サービスの堅牢化
  - BIND デーモンの "chroot" jail 構成
    - プロセスを一部のファイルシステムのみアクセス可能
      - /var/jail/bind ディレクトリの作成、必要なファイルのコピー
      - finish-named-chroot.sh スクリプトの作成
  - Non-root ユーザでの BIND デーモンを構成
    - named ユーザの作成

HP-UX Bastille's Apache and FTP Modules

- Apache の堅牢化(hardening)
  - 不必要であれば、Apache デーモンを停止
  - Apache が実行できるよう“chroot” jail 構成
- FTP 設定
  - システムアカウント(root, daemon, bin, sys, adm, uucp, lp, nuucp, hpdb, guest)ユーザでのFTPアクセスできないよう設定

HP-UX Bastille's HP-UX Module

- カーネルベースのスタック実行保護機能を有効
  - カーネルパラメータの変更(executable_stack を 0)
- リモートからの swlist を制限
  - swacl コマンドで ACL を変更(any_other:-r--- を削除)
- ネットワーク調整パラメータの変更
  - ip_forward_directed_broadcasts(0)
  - ip_forward_src_routed(0)
  - ip_forwarding(0)
  - ip_ire_gw_probe(0)
  - ip_send_redirects(0)
  - ip_send_source_quench(0)
  - tcp_conn_request_max (20 -> 4096)
  - tcp_syn_rcvd_max (500 -> 1000)

HP-UX11iスタックの実行保護 (Buffer overflow protection)

システムへのセキュリティ攻撃として一般的なバッファオーバ攻撃への防御機構を提供

- プログラムスタックのオーバフローによるスーパユーザ特権での実行を監視

  WARNING: UID # may have attempted a buffer overflow attack. PID # (program_name) has been terminated. See the '+es enable' option of chatr(1).

- 監視対象アプリケーションの修正は必要なし
- アプリケーションへの影響を確認できる「トライアル・モード」を実装
- 正当なアプリケーションに影響を及ぼさないようアプリケーション毎の適用・非適用を選択が可能
  (ゾーン・バイパス機能)

HP-UX Bastille's IPFilter Module

- IPFilter による基本的なファイアウォールの設定
  - 明示的に指定された以外の受信パケットをすべてブロック
  - 送信パケットは、ブロックしない
  - 主なサービスの受信パケットの設定
    - Secure Shell リモートアクセス
    - WBEM マルチシステム管理
    - HIDS (Host Intrusion Detection System) エージェント
    - web 管理ツール
    - DNS 検索およびゾーン転送
  - 環境に応じたルール設定が可能
    /etc/opt/sec_mgmt/bastille/ipf.customrules

Webサーバへのアクセスのために受信ポート80番へのコネクションを許可する記述例

pass in quick proto tcp from any to any port = 80 keep state

Bastille トラブルシューティング

- /var/opt/sec_mgmt/bastille/log/action-log(ログ)
- /var/opt/sec_mgmt/bastille/log/error-log(エラーログ)
- /var/opt/sec_mgmt/bastille/TODO.txt (手動設定リスト)
- /etc/opt/sec_mgmt/bastille/config

```
# Q:  Do not allow logins unless the home directory exists?
AccountSecurity.ABORT_LOGIN_ON_MISSING_HOMEDIR="Y"
# Q:  Should non-root users be disallowed from logging in if /etc/nologin exists?
AccountSecurity.NOLOGIN="Y"
```

- ファイアウォール設定：
  - /etc/opt/sec_mgmt/bastille/ipf.customrules
  - /etc/opt/ipf/ipf.conf
- 設定前の状態に戻す(bastille -r)
  /var/opt/sec_mgmt/bastille/TOREVERT.txt

hp-ux11i セキュリティ脆弱性への迅速な対応

既知のソフトウェアセキュリティ脆弱性に対する対応は エンタープライズ・システムのセキュリティ強化において非常に重要

- セキュリティ脆弱性状況の監視
  CERT/CC などセキュリティ監視組織との協調
  (http://www.cert.org/)

- セキュリティ脆弱性と対応情報の迅速な提供(ITリソース・センタ)
  - 英語による迅速な情報提供
  - 日本語によるダイジェスト（概要）の提供

- セキュリティ・パッチの適用（インストール）支援ツールの提供

関連資料

- 『HP-UX 11iシステムセキュリティ』
- 『stack buffer overflow protection in HP-UX 11i』
  - http://www1.jpn.hp.com/products/software/oe/hpux/document/index.html

- 『HP-UX システム/ワークグループの管理』
  8. システム管理：システムの安全運用の管理
  - http://docs.hp.com/ja

- ITリソース・センタ
  - http://www.itrc.hp.com

- Security bulletins Digest 日本語版
  - http://www3.jpn.hp.com/upassist/assist2/secbltn/index.htm