仙台 CTF 2017

調査用仮想マシン「Caine」の操作方法

平成29年11月12日

仙台 CTF 実行委員会

フォレンジック用 Linux「Caine」をインストールした Virtual Box 形式仮想マシンを準備しました。

「Caine」には、セキュリティ技術勉強会の実習で使う「Volatility Framework」、「Plaso/log2timeline」をはじめ、さまざまな調査ツールがインストールされていますので、ツールのインストールが失敗してしまう場合などにご活用ください。

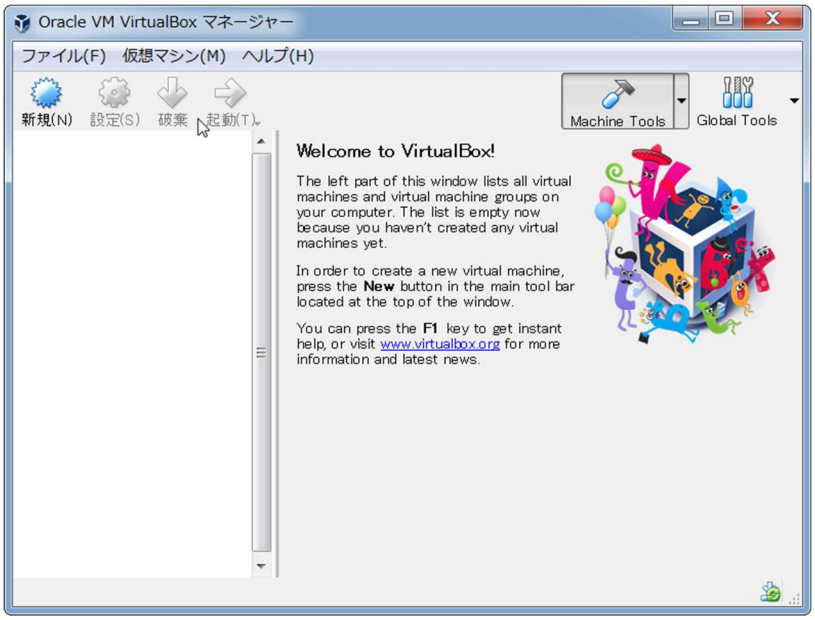
利用方法

Windows 版 Virtual Box の操作方法を説明します。(Mac 版も操作方法はほぼ同じです。)
なお、事前に、仙台 CTF 特設サイトからダウンロードした仮想マシンのイメージファイルを任意のフォルダに展開してください。

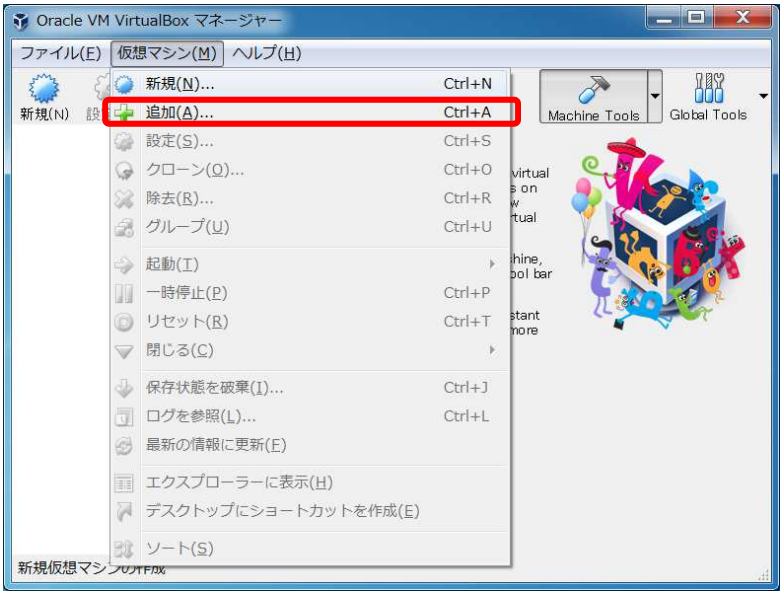
1. Virtual Box の公式サイトから、ご利用の OS 用のインストーラーをダウンロードし、インストールします。インストーラーはウィザード形式となっておりますので、画面の指示に従い操作してください。

   Oracle Virtual Box 公式サイト
   http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html?ssSourceSiteId=otnjp

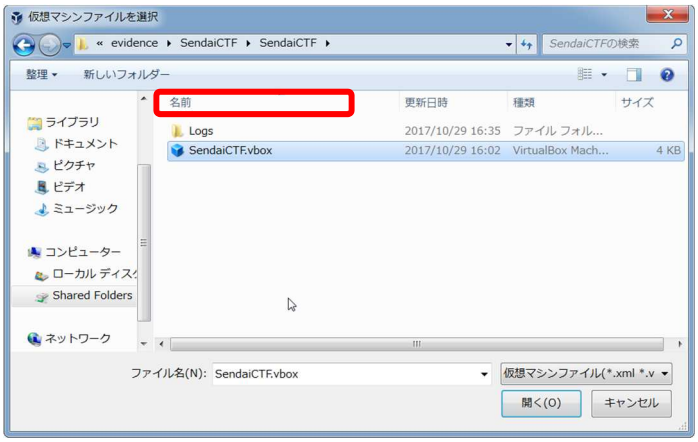
2. インストールした Virtual Box を起動します。



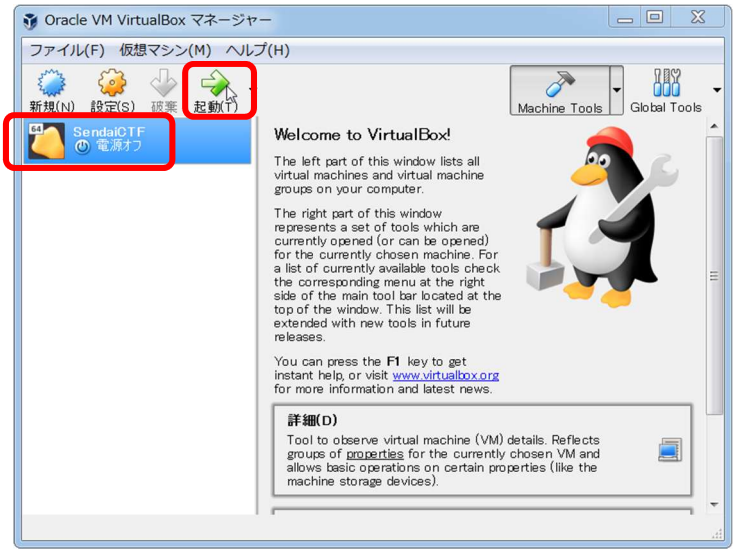
3. 「Oracle VM Virtual Box マネージャー」のメニュー「仮想マシン」ー「追加」を選択します。



4. 事前に展開しておいた「Caine」の仮想マシン（拡張子.vbox）を選択します。



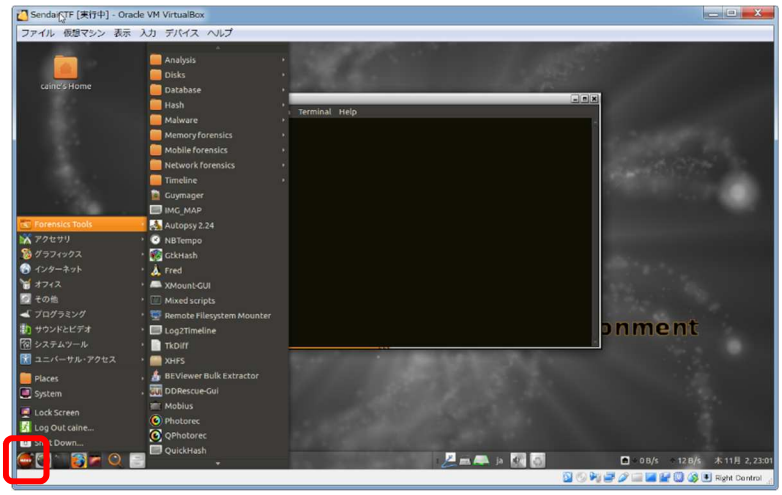
5. Virtual Box に読み込んだ仮想マシンを選択のうえ、「起動」アイコンをクリックし「Caine」を起動します。なお、起動途中の画面でいくつかエラーメッセージなどが表示されますが、無視して構いません。



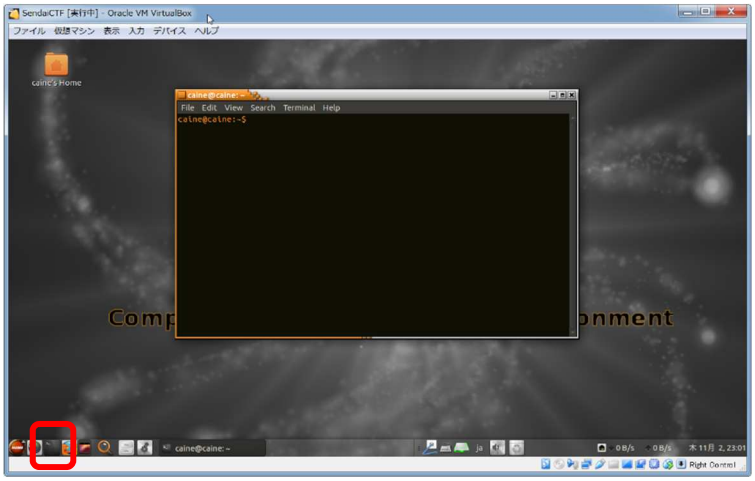
6. 「Caine」の起動メニューが表示されたら、キーボードのエンターキーを押して起動処理を進めます。

7. しばらくすると、「Caine」のデスクトップ画面が表示されます。

8. 画面左下の「MENU」ボタンをクリックすると、メニューが表示され、ツールの起動やシャットダウンなどの操作を行うことができます。



9. ターミナルアイコンをクリックすると、コマンドプロンプトが起動されます。
セキュリティ技術勉強会で利用するツールは、「volatility」、「log2timeline.py」、「plaso.py」という名前で起動することができます。



TIPS-1 仮想マシンから抜け出す方法

仮想マシン（ゲスト OS）にキー入力が奪われて、ホスト OS の操作ができなくなった場合は、「ホストキー」を押すことで抜け出すことができます。「ホストキー」は、Windows 版では「右側の Ctrl キー」、Mac 版では「左側の Command キー」に割り当てられています。

また、「ホストキー」と「F」を同時に押すと、仮想マシンを全画面表示に切り替えることができます。全画面表示を終了したい場合は、再度「ホストキー」と「F」を同時に押してください。

TIPS-2 ホスト OS 側のフォルダを「Caine」と共有する方法

Virtual Box の「共有フォルダー」機能を使うと、ホスト OS の任意をフォルダを、仮想マシン（ゲスト OS）側からアクセスできるようになります。操作手順は次のとおりです。

（1）「Oracle VM Virtual Box マネージャー」の「設定」アイコンをクリックし「設定」ダイアログを表示し、「共有フォルダー」を設定します。（ここでは、「share」というフォルダ名で共有を作成したものとします。）

（2）設定した共有フォルダを「Caine」で利用するためには、「Caine」のコマンドプロンプトからマウントコマンドを実行します。

```
$ sudo mount -t vboxsf  share  /mnt
```

（3）上記のコマンドにより、仮想マシン側のディレクトリ「/mnt」に、ホスト OS 側の共有フォルダがマウントされます。

以上