# 保全演習手順書

# 内容

# 1 保全

ここでは保全を行います。

本実習では予め保全されたデータを使って調査を行いますが、保全手順の確認のみ行います。

## 1 - 1 データ保全

コンピュータのデータは時間の経過とともに失われてしまうため、サイバー攻撃を受けた時は、始めに調査対象となるコンピュータのメモリやハードディスクの情報を保全します。失われやすいメモリのデータを保全し、その後にハードディスクのデータを保全します。調査や解析は保全したデータを使って行います。メモリやハードディスクのデータを保全するに十分な空き容量のあるハードディスクが必要です。

### 1 - 1 - 1　メモリイメージの保全

保全手順の確認には、仮想マシン「04_TargetPC」を使用します。

デスクトップの「Oracle VM VirtualBox」アイコンをダブルクリックして、VirtualBox を起動し、「04_TargetPC」を起動します。

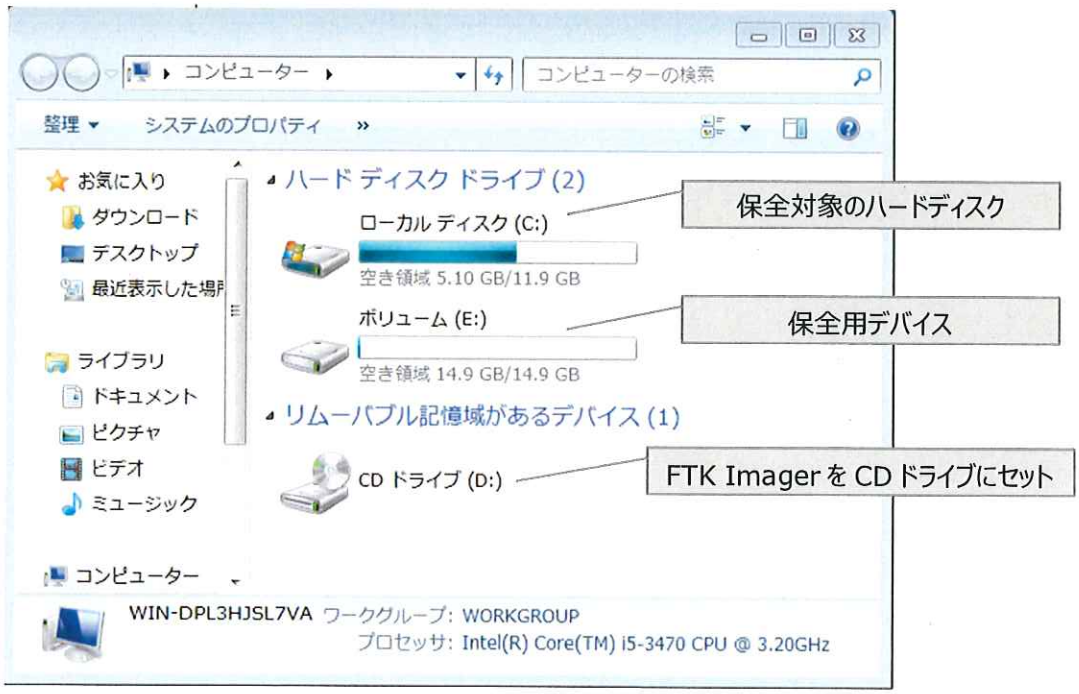
仮想マシン「04_TargetPC」に、ユーザー「joy」、パスワード「P@ssw0rd」でログオンします。

以下の前提で保全手順を確認します。

・保全対象　　メモリ　および　内蔵ハードディスク(C ドライブ)

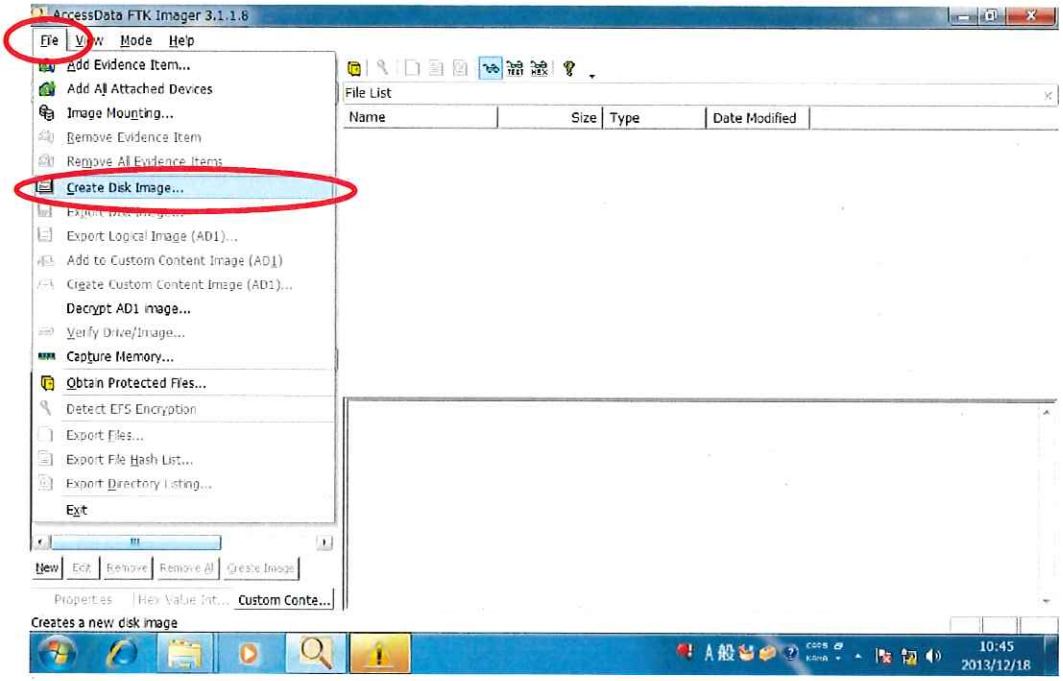
・保全用デバイス　　外付け USB ハードディスク(E ドライブ)

・保全用ツール　　FTK Imager Lite (CD-ROM)

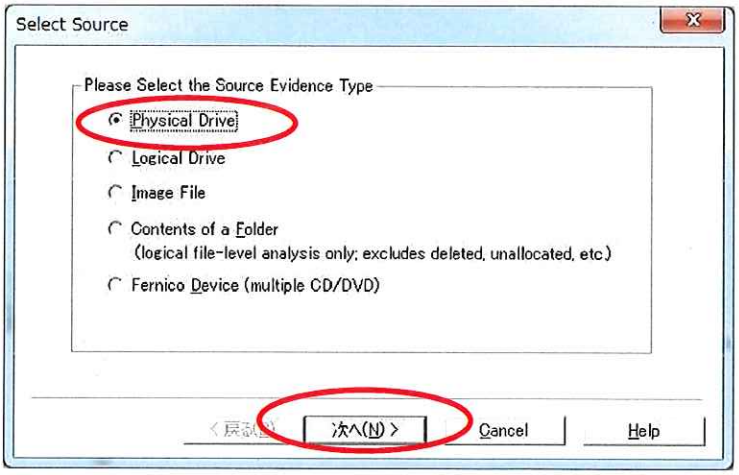


### 1-1-2 ディスクイメージの保全

次にハードディスクの内容を保全します。[File]-[Create Disk Image...]メニューをクリックします。




保全対象ディスクのタイプを選択します。ハードディスク全体を保全するため、[Physical Drive]を選択します。



## 1 - 2 対象システムの停止

被害の拡大を防止するため、データ保全を行ったのちは対象システムをシャットダウンするか、もしくはネットワークから切り離します。
本実習は仮想環境のため、対象の仮想マシンをサスペンド状態にします。