実践セキュリティ特論 上原先生 第三回課題

28G23027
川原尚己

問 1：SSD において全セクタのイメージ作成による証拠保全が効率が悪い理由を説明せよ.

SSD は電気的な状態によって情報の保持を行っており，しばらく使わないでいると電荷がだんだんと失われ，データが消えて行ってしまうため.

問 2：自己暗号化ドライブ（SED）の利用はどのようにストレージの廃棄を効率化するか,またその場合に残ると考えられるリスクは何か説明せよ.

暗号化に使用した鍵を廃棄することでデータを消去できる．鍵はコマンドを入力するだけで消去できるため，非常に素早く，かつ安全に消去をすることができる．ただし，鍵を完全に消去しなければ，データを復元できてしまうため，バックアップを含めすべての鍵を消去しなければならない.

問 3：フォレンジックにおいて最近ライブ・フォレンジックが重要となってきた理由について説明せよ.

主記憶装置上のみで動作するマルウェアであるファイルレスマルウェアが出現している．ファイルレスマルウェアは一度シャットダウンすると二度と再現することができないため，動作中の主記憶の内容をできるだけ保全しておく必要があるから.