

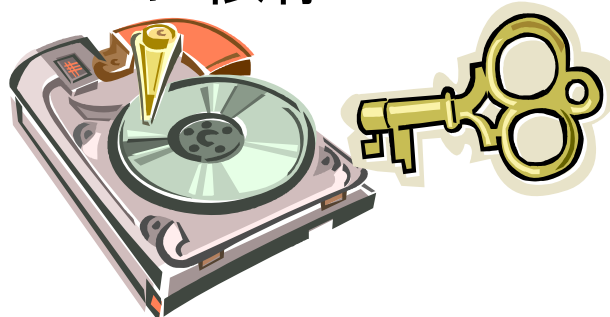
第二回 調査技術ゼミ
2005年9月05日

『 暗号化とフォレンジック調査 』
ハードディスクパスワード

ネットエージェント株式会社

ハードディスクパスワードとは

- ハードディスクにパスワードを設定し、プリブート認証を行う。
- ATAコマンド “Security Set Password” にて動作
 - 限られた一部のコマンド以外、データアクセスを受け付けない
 - 実装はプラットフォームに依存？



検証：ハードディスクパスワード

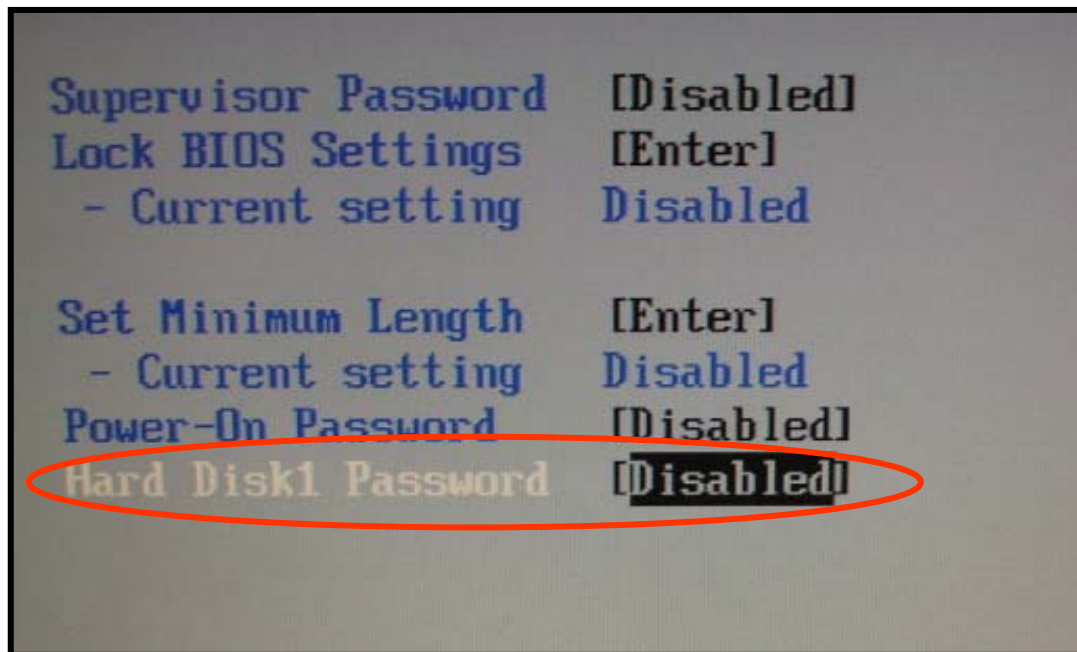
環境：IBM ThinkPad R40e 2684-HHJ

- ・ 検証1：パスワードを設定しOSを起動
- ・ 検証2：KING DEMI-Forensicで物理コピー



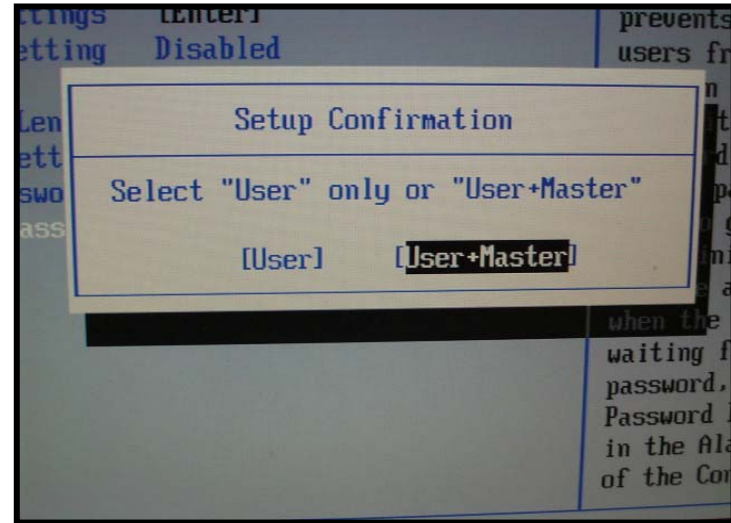
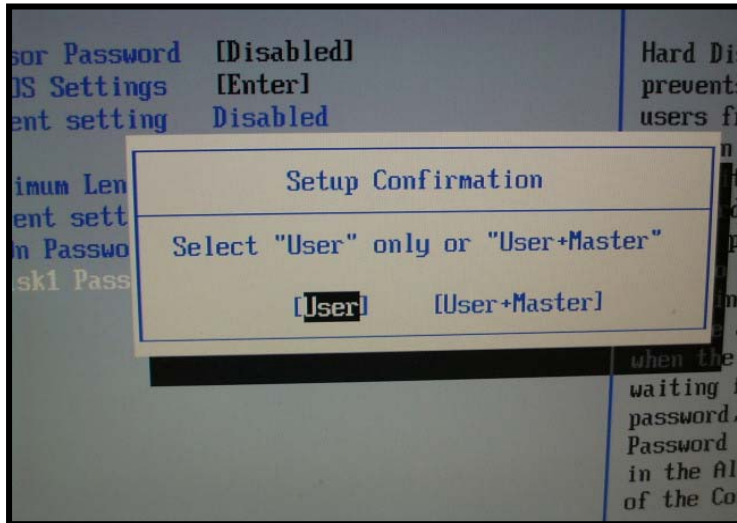
検証1:ハードディスクパスワードの設定

- ・ bios起動後、Security設定画面に遷移し、Hard Disk Passwordを実行



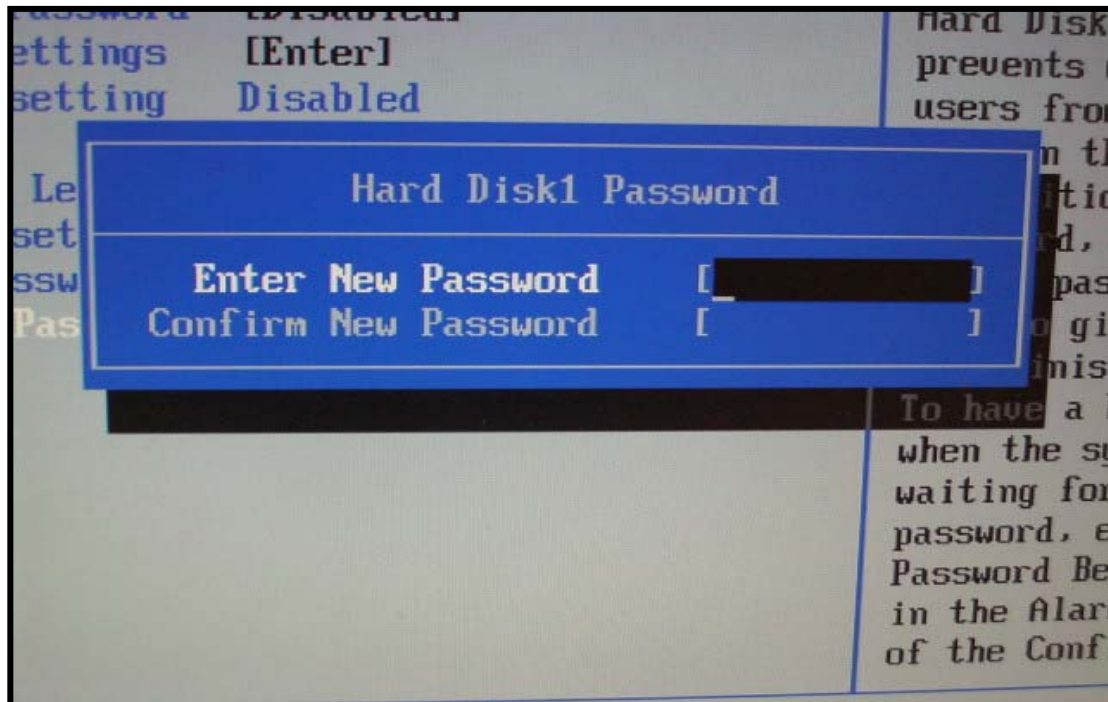
検証1:ハードディスクパスワードの設定

- ・ Userもしくは、User+Masterのハードディスクパスワードを設定



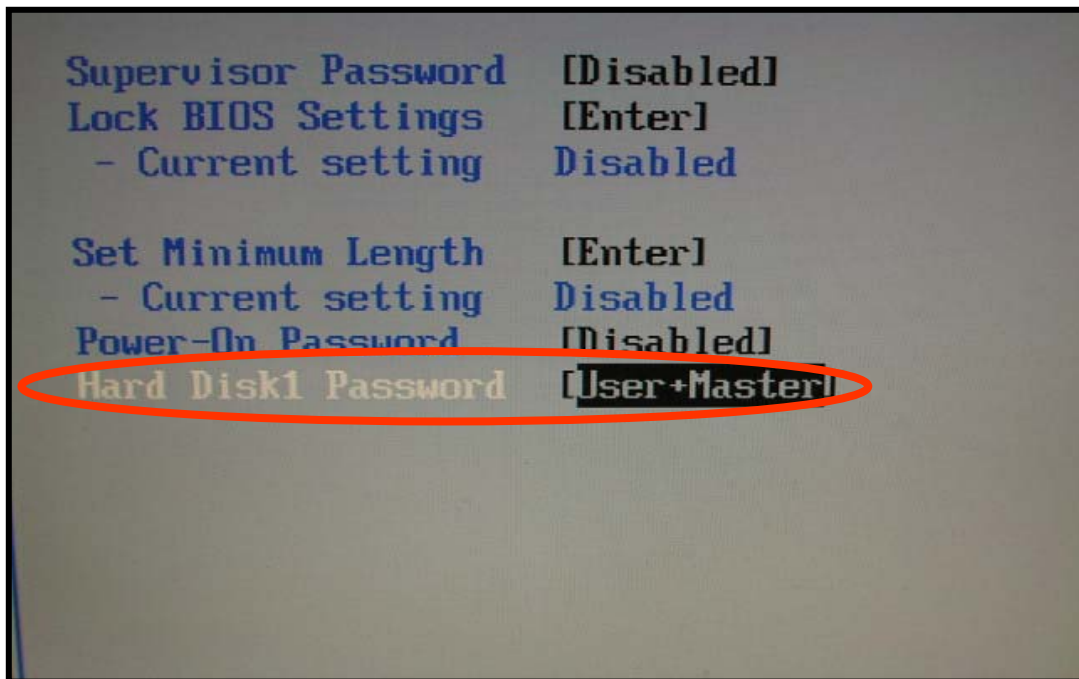
検証1:ハードディスクパスワードの設定

- パスワード設定



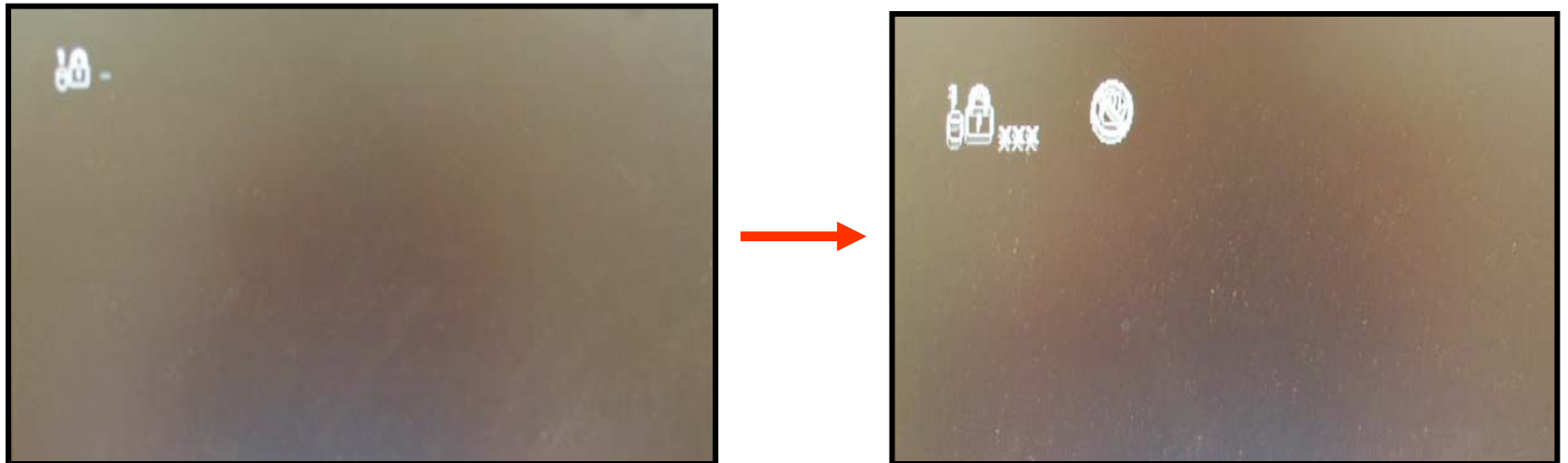
検証1:ハードディスクパスワードの設定

- Hard Disk Password設定終了



検証1:ハードディスクパスワードの設定

- 再起動後の状態。パスワードを入力するまでOSは起動しない。
 - 3回認証に失敗するとロックされる(プラットフォームに依存)



検証2: パスワード設定されたディスクを KING DEMI-Forensicで物理コピー

- ThinkPad R40e 2684-HHJからハードディスクの取り出し



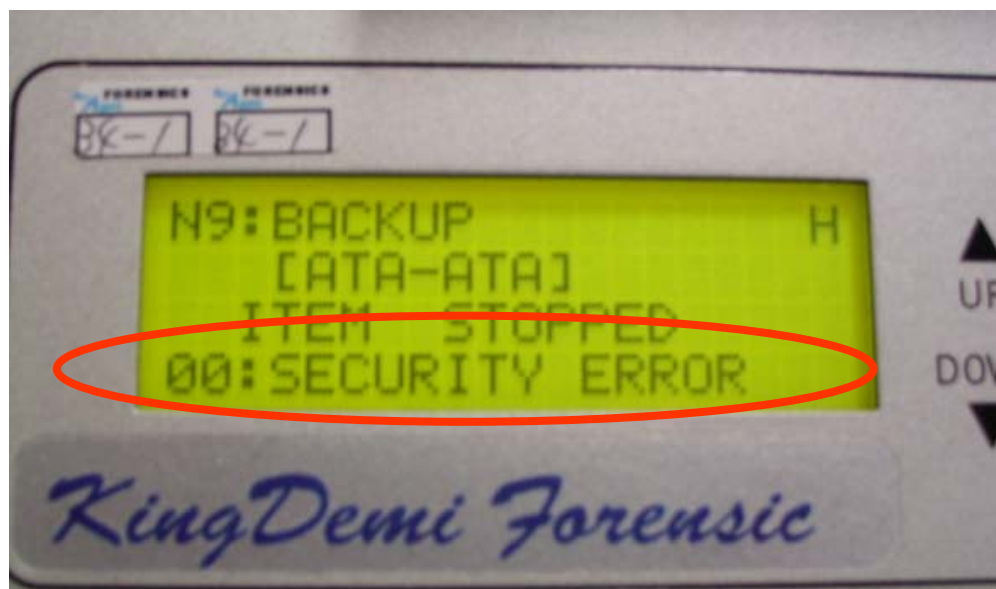
検証2: パスワード設定されたディスクを KING DEMI-Forensicで物理コピー

- ・ KING DEMI-Forensicに接続し、物理コピー
- 2.5インチ変換アダプタ使用



検証2: パスワード設定されたディスクを KING DEMI-Forensicで物理コピー

- ・ コピー開始数秒後に、SECURITY ERROR
で終了
 - コピーの種類によっては暴走の危険がある



検証2: パスワード設定されたディスクを KING DEMI-Forensicで物理コピー

- ・ SECURITY ERROR

- エラー内容:

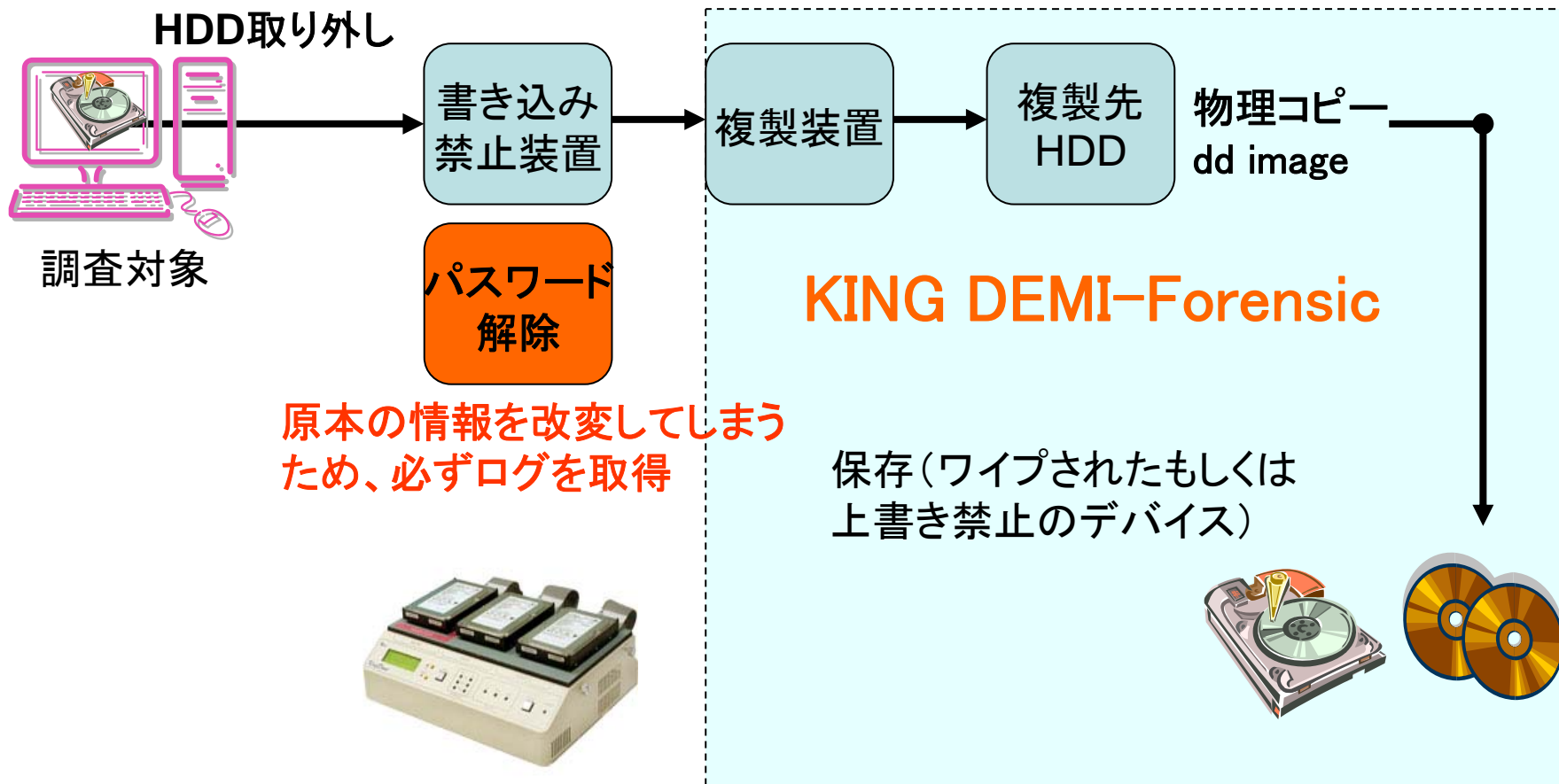
- ・ SECURITY LOCKされているHDDが接続された時に表示されます。

- 対処方法:

- ・ そのSECURITY LOCKを解除してください。SECURITY LOCKを解除しない場合、そのHDDを使用することはできません。

- YEC KING DEMI AS FOREMSIC版テクニカルマニュアルP39「装置が発行するエラー」表より引用

パスワード設定されたディスクでの 証拠保全の流れ



ハードディスクパスワードを解除するには (管理的手法)

- ・ ユーザパスワードとマスターパスワード
 - パスワードを入力し、ロック解除
- ・ スーパーバイザーパスワード
 - 機種によってはハードディスクパスワードを上書きできるものもある(DELL等)

ハードディスクパスワードを解除するには (技術的手法)

- ・ 技術的には、ハードディスクパスワードをかけたものは解除できないというのが定説だが・・・
 - ツールでデータを解析してしまえば？
 - 秋葉原へ！！
- (株)UBICが販売している Password Cracker POD も・・・
 - 法執行機関、政府関連機関に対してのみ販売

<http://www.ubic.co.jp/VOGON-Pod.html>

アンチフォレンジック手法としての ハードディスクパスワード

- ・ 情報セキュリティ犯罪を隠蔽する手段としてのハードディスクパスワード
 - 技術的に解析するのは困難(コスト、時間的制約)

biosを含めて、マシンを適切に管理し、デバイスの設定変更を自由にさせない管理が重要



参考

- ATA/ATAPI-7 revision 4b Vol. 1
 - <http://www.t13.org/docs2004/d1532v1r4b-ATA-ATAPI-7.pdf>

**解き明かす力、今すぐにでも。
フォレンジック・サービス**

NetAgent

The Forensics Company

<http://forensic.netagent.co.jp/>