平成23年度 卒業論文

論文題目

個人情報漏えいを防止するための
モバイル機器のセキュリティ対策と検討

神奈川大学 工学部 電子情報フロンティア学科

学籍番号　200803001

田中　友之

指導担当者　木下宏揚　教授

目 次

図 目 次

第1章

序論

今日、モバイル機器の普及にともない情報漏えいなどが社会的に大きな問題になっている。これは、私たちが様々なモバイル機器を使用し個人情報を持ち歩いている一方で、セキュリティの知識がないことが原因である。震災後はテレワークが増え、外部に情報が流れるケースが急増している。

本研究は、モバイル機器のセキュリティが保たれる扱い方を検証・評価し、ガイドライン規定を作成するために必要となるモバイル機器のセキュリティ問題を体系化し、情報漏えいの防止対策に役立てることを目的とする。
情報漏えいの原因として以下の 3 つがあげられる。
(1) ストレージ内にウィルスが侵入（盗聴、ハッキング）
(2) ストレージからの直接的な情報漏えい (紛失, 廃棄, ハイバネーション)
(3) ストレージに対するアクセス未制限（個人情報が入っているフォルダを自由に閲覧可能)[22]

本研究ではこれら (1)(2) の原因の対策を評価、検討している。

第 2 章では PC から情報が流失する原因、第 3 章では暗号化ソフトについて考察し、1 台の PC の中で業務用と私用 (もしくは別の業務) をしなければいけない場合のウィルス感染や情報漏えいの対策を検討しその安全を評価する。第 4 章では HHD に代わる SSD の廃棄時のデータ消去について述べる。

第2章

情報が流失する原因

2.1　情報が流出する原因

PCから情報が流出するルートは大きく二つに分けられる。一つ目はコンピュータウィルス感染によるインターネット経由での流出、二つ目はノートPCなどの盗難・紛失などにより物理的に流出するケースである。[22]

2.1.1　コンピューターウィルス

コンピュータウィルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムで、感染すると何らかの弊害が発生する。弊害というのは、メッセージや画像を表示するだけのものもあるが、危険度が高いものの中には、ハードディスクに格納されているファイルの消去や、コンピュータを起動できないようにするもの、パスワードなどのデータを外部に自動的に送信するタイプもある。[26]

一般的に流通しているウィルスは以下の様な特徴を持っている。

- **ワーム** インターネット経由であるコンピュータに感染し、その感染したコンピュータのネットワークを通り、ネットワークにつながる全PCに攻撃をしかけ、セキュリティホールを発見し感染を拡大していく。[26]

- **トロイの木馬** 自らを有益なソフトウェアであるとユーザーに信じ込ませ、実行するように仕向けるウィルスである。これに騙され実行してしまうと、PCにウィルスが侵入し、データを消去したり、外部に流出させたりする。実行した途端活動を始めるものもあるが、システムの一部として潜伏し、時間が経ってから発症するものや、攻撃者がそのPCを乗っ取るための窓口として機能するものもあり、ユーザーがそれをウィルスであると認識し難いこともある。[26]

- **スパイウェア** インターネットでフリーソフトをインストールする際に、一緒にこのウィルスも入り込み、PCの動作を不安定にする。すでに紹介した二つのウィルスと異なる点は、ユーザーの承認を受けてインストールされるということである。[26]

このようにウィルスの多くはインターネット経由でPCに侵入する。また、インターネット経由でウィルス感染したPCでデータをUSBメモリに保存し、そのUSBメモリを別のPCに接続しデータを扱うことで感染が広がる場合もある。ウィルス拡大の要因として、ファイル共有ソフトも挙げることができる。ファイル共有ソフトとは、インターネットを利用してP2Pでファイルをやり取りするソフトウェアである。ユーザーは、インターネットに接続された自分のコンピュータに、ファイル共有ソフトを導入することで、他のユーザーとファイルをやり取りすることができるようになるが、このソフトは自動的にPC上の全てのファイルを送受信する仕組みであるため、公開するつもりのないファイルが公開されてしまったり、ウィルスが不特定多数のユーザーに流れてしまったりすることもある。

2.1.2 物理的な情報流出

二つ目に情報が流れるルートとして、ノートPCの盗難や紛失などによる物理的流出があげられる。こういった場合に備えた最低限の対策として、また一つのPCを複数のユーザーで共有する場合のユーザー認証としてログインパスワードを設定する。一般的なパスワードの強度は、英数字だけを使用した場合の12文字以上が中、14文字以上が強、28文字以上が最強であるとされる。解析ソフトなどを使いパスワードを解析すると、5文字程度であれば私たちが使用している個人用パソコンでも1日ほどでパスワードを破ることができてしまう。対策として1〜2ヵ月おきにパスワードを変更し、可能な限り14文字以上で設定する。[22][29]

ログインパスワードを設定していても、様々な要因によって危険度が異なる。その要因としてあげられるのが以下の4点である。

- **電源**

  PCの電源の状態によっても危険度の差異がある。
  まず、電源をつけた状態でPCが盗難にあった場合は、ほとんどの場合対策を立てていても個人情報の流失を防ぐことが出来ない。次に、ハイバネーションという状態がある。これは、PCの電源を切る直前の状態を保存して、次に電源を入れたときに電源を切る直前の状態から作業を再開する機能であり、休止状態とも呼ばれる。ハイバネーション状態ではメモリの内容がハードディスクに保存され、再開時にはその情報がメモリへと復元されるので、ログインパスワードを設定していない場合電源をつけた状態と何ら変わらない状態になってしまう。スリープモードはWindows Vistaから標準装備された機能であり、スタンバイと休止状態を組み合わせた省電力モードであるが、単に省電力になったというわけではない。Windows Vistaでは、スタート・メニューのシャットダウンのボタンは正確にはスリープモードであるが、アプリケーションは終了されるため、電源が切れているのと同じ状態であるので問題はない。[30]

- **ハイバネーション**

  ハイバネーション状態については前項目で述べたが、ハイバネーション状態のデータ保存方法も問題があると言える。ハイバネーションの場合は作業中のデータをハイバネーションファイルとしてハードディスクに保存する。ハイバネーションファイルには一時停止した時点でのメモリ内容のスナップショットが保存されるので、休止状態のPCからハイバネーションファイルを抽出して調査することにより、その時点でどのようなプロセスが動いていたか、また各プロセスがどのようなデータを持っていたかを知ることができる。

  ファイルを暗号化していれば、PCが盗難に遭ったとしてもハードディスク上のファイルから情報が漏えいする可能性は極めて低くなる。しかし、ハイバネーションファイルは通常メモリ中にはデータは復号して格納されるので、元のデータが暗号化されていても平文で保存される。つまり、暗号化していたつもりの情報が、ハイバネーションファイル経由で漏えいしてしまう危険がある。[18][24]

- **テンポラリファイル**

  ハイバネーションファイルと同様に、テンポラリファイルも情報漏えいの危険があると言える。テンポラリファイルは、ソフトウェアが作業中のデータの保存のために一時的に作るファイルであるので、一時ファイルとも呼ばれる。閲覧したインターネット履歴、編集中のファイルの自動バックアップなど、様々な用途に使われる。ほとんどの場合、ソフトウェアの終了と同時に消去されるがPCがフリーズしたり、アプリケーションが正常終了しなかった場合、一部のデータが残ることがある。一時ファイルに保存された個人情報の入った編集中のファイルなどが流出してしまう恐れがある。シャットダウンする前に手動で一時ファイルを削除することで安全性を高められる。[25][26]

- **メモリ**　OSがプログラムを実行・管理する際にプロセスが生成され、メモリに一時的に保存される。OS上で生成されたプロセスには、仮想アドレス空間が割り当てられ、それぞれのプロセスは独立したものである。あるプロセスから別のプロセスの仮想アドレス空間にアクセスすることはできない。よって、あるプロセスがウィルス感染したとしてもメモリ全体が感染することはない。

  しかし、物理的にアクセスできる状態を作ってしまうとログインパスワードを設定しているPCに対しても、DV端子経由でメモリにDMA(ダイレクトメモリアクセス＝CPUを介さずに各装置とRAMの間で直接データ転送を行う)することにより、直接メモリ内のプログラムコードを改変してパスワードロックを解除するという攻撃手段も存在する。[17][19][20][21][31]

2.1.3 その他の危険性

本章の冒頭で、情報流出のルートは大きく二つに分けられると述べたが、その他の危険性も指摘しておかなければならない。

- **バッファオーバーフロー**確保したメモリ領域（バッファ）を超えてデータが入力された場合に、データがあふれてプログラムが暴走してしまうことをバッファオーバーフローと言う。バッファオーバーフロー攻撃は、バッファに対して許容量を超えるデータを送り付け、システムを機能停止にしたり、あふれ出たデータを実行させ、セキュリティホールを作り出す。このセキュリティホールを利用し、ウィルス感染を容易にさせる。

  バッファオーバーフローは最も代表的なセキュリティホールであり、現在OSで見つかっているセキュリティホールの半数以上はこれによるものといわれている。

  対策として常にPCを最新版にしてくことや不要なネットワークアクセスを制限、使っていないサービスプログラムを停止することが有効である。[32]

これらの情報流失を防ぐ対策を次章から述べていく。

第3章

仮想化と暗号化

3.1 仮想化

1台のコンピュータをあたかも複数台のコンピュータであるかの様に、それぞれに別のOSやアプリケーションソフトを動作させることができる。これを仮想化と言う。仮想化のメリットとして次の3点が挙げられる。
(1)パーティショニング＝１つのストレージを分割し、同時に複数の仮想PCを実行できる
(2)隔離＝同じハードウェア上の仮想PC同士を完全に独立状態で稼働できる
(3)カプセル化＝ハードウェア構成、Bios、ディスクの状態など仮想PC全体を物理ハードウェアから独立したファイルに保存できる。[2][4][5][6]

この仮想化を情報漏えいののセキュリティ対策として用いることが出来ないかを検討する。

3.1.1　仮想化ソフトの種類と特徴

仮想化を行うためのソフトの特徴を簡潔に述べると以下の通りである。

- **VMware Player**

  仮想マシン稼働の環境に特化したソフトである。構築済みの仮想マシンを手軽かつ高速に稼働できる。しかし、仮想 PC の新規作成や設定変更機能などは備わっていない。仮想化ソフト初心者には導入も使い方も簡単である。[1][7]

- **Virtual PC**

  一台のコンピュータ上で仮想的に複数台のコンピュータが動作可能になり、仮想化されたそれぞれの仮想マシン上ではそれぞれ別の OS を同時に動作させることができる。バージョンによっては USB 機器の認識が未対応であったり、OS が Linux では作動できない場合がある。[1]

- **Virtual Box**

  Virtual PC と同様に PC 上に仮想 PC を作成し、別の OS を実行できる。Virtual PC との違いは、USB 機器を利用できる上、リモートデスクトップ接続ができるなど独自の機能も備えている。対応の OS は Windows、Mac、Linux、FreeBSD と幅人い。[28]

本研究の提案モデルでは 1 台のホスト PC 上に 2 台の仮想 PC を設定し一般ユーザが主に使用する windows や Mac といった OS で使用でき、仮想 PC 上で USB 機器の使用も可能という利点から Virtual Box を使用する。

3.2 暗号化

暗号化とは第三者に通信内容や保管書類を読み取られないようにパスワードや鍵を掛け、それらを解かなければ中の内容を見ることが出来ない仕組みのことである。ノートPCや、USBメモリなどを持ち運び、万が一誰かの手に渡ってしまうことを考え、中の情報を暗号化しておくことで、パスワードなどによる認証を破られない限り、情報の流出を防ぐことができる。[3][16]

3.2.1 暗号化ソフトの種類と特徴

暗号化にも一般的に用いられるソフトは以下の通りである。

- **EFS**

  Windows2000/XPの標準ファイルシステムであるNTFSが持つファイル暗号化機能である。ファイルやフォルダに属性として設定され、暗号化属性が付加されたファイルはディスク上に暗号化された状態で記録される。暗号化されたデータは暗号化を行ったユーザしか復号できないため、他に同じファイルにアクセス権を持つユーザでも、データを復号できないために事実上アクセスが不可能となる。暗号化を行ったユーザが所属するPCの管理者は例外的にデータを復号できる。[11][12]

- **TPM**

  TPM=Trusted Platform Module は耐タンパ性 (物理的あるいは論理的に内部の情報を読み取られることに対する耐性) を持ったチップである。

  データの暗号化や復号など、その際に用いる鍵情報を保持する機能を持ち、PC などのマザーボード上に取り付けられている。これにより PC において機器認証とプラットフォーム認証 (ソフトウェアやハードウェアを動作させるための基盤となるハードウェアや OS との認証) ができるようになる。ハードディスクのデータやパスワードを暗号化して保存する際などに利用することで、暗号化に利用したチップとセットでないとデータを読み出せなくなっている。これにより、ハードディスクだけ盗まれたとしても、中のデータの暗号を解くことができなくなる。しかし、OS の管理外の不正なディスクの読み取りを制限することはできるものの、TPM のみでは、OS 起動に対する追加のセキュリティを得ることは出来ない。[26]

- **Bitlocker**

  初めに挙げた EFS はファイル単位の暗号化機能であったが、Bitlocker はディスクの暗号化である。前述の TPM と連携し、ハードウェアレベルでデータ漏えいを防ぐことができる。PC にパスワードをかけていても、PC ごと盗難にあった場合には、ハードディスクを取り出され、読み取られてしまうことがある。これを防ぐために、ハードウェアに固有のキーを使ってハードディスクの内容を暗号化し、不正な手段でのデータ読み取りを不可能にするのが BitLocker の機能である。また、データ読み取りだけでなく、不正な改ざんなども検知し、データを保護することができる。BitLocker では、OS のインストールされたボリュームのみを暗号化するため、他のボリュームに関しては、従来の暗号化ファイルシステムを用いる必要がある。

  しかし、Bitlocker は，Windows Vista Ultimate または Windows Vista Enterprise でしか使用できないため個人利用には不適切である。[11][15]

- **True Crypt**

  TrueCrypt は無料で使用できる暗号ソフトであり、暗号化された仮想ディスクを作成・利用することができる。仮想ディスクはファイルとして作成するだけでなく、パーティション自体も対象にできる。Windows 版 TrueCrypt ではシステムドライブ自体も暗号化することが出来る。

  パソコンを紛失し、万が一ハードディスクからデータを引き出されそうになっても、暗号化されていることで防止することができる。また、マウントした仮想ドライブへアクセスすると、自動で暗号化・復号を行うので、ユーザは暗号化／復号を意識する必要がなく暗号化ソフト初心者に最適である。[24][26]

  無料でダウンロードでき、ドライブ全体の暗号化を行える点を考慮し、本研究の暗号化にはこのソフトを利用している。

3.2.2 EFSの有効性

上記のように、EFSはドライブを対象としたものではなく、フォルダーとファイルが対象である。

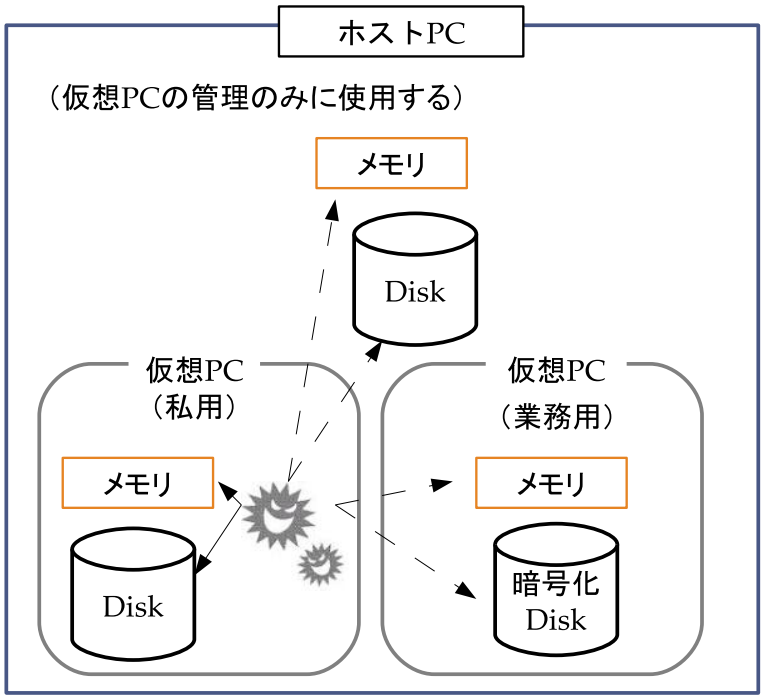
設定方法は容易であるが、OSのあるHDDの中には、ユーザーの秘密鍵が入っているので、PCをの起動時にパスワードなしで自動ログオンできるようになっていると、EFSによる暗号化は全く意味がなくなってしまう。
よってログオン・スタンバイ・休止状態からの復帰には必ずパスワードが必要である。
EFSの使用例としては1台のパソコンで何人ものゲストユーザーが使用する際に、ホストユーザーが共有したくないファイルをEFSで暗号化することで、ゲストユーザーはこのファイルを開くことが出来ない。また、すべてのユーザーがホストであっても他のホストユーザーのEFSで暗号化されたファイルを閲覧することもできない。EFSは持ち出すパソコンには不向きであり、OS内に秘密鍵があることから暗号化の強度としては低いものと言える。[11][12]

3.2.3 BitlockerとTrueCryptの有効性

TrueCryptと、TPMを併用したBitlockerではどちらが有効であるのか。TrueCryptは攻撃者がPCに物理的にアクセスした後に、正規ユーザーがPCにアクセスした場合はデータを守ることを保証できないとしている。例えばホテルの部屋などに、TrueCryptでディスクを暗号化したノートPCを宿泊客が置いていると想定し、その部屋に侵入した人物が、攻撃コードを仕込んだUSBメモリを設置する。その後宿泊客がPCを起動する際、ディスク暗号化のパスフレーズを読み取る不正コードが感染する。読み取られたパスワードはネットワーク経由で外部に送信されるといったものである。これに対してTPMはブートローダを書き換える攻撃を検知できる。つまり、TrueCryptはブートローダ自体を暗号化していないのでブートローダの改変には対処できないが、TPMはそれを防ぐことができる。しかし、TrueCryptでもディスク全体を暗号化し、Biosパスワードを設定すればセキュリティは向上する。BiosパスワードはPCの起動時にパスワードを入力しないと起動できないようにする機能である。マザーボードに組み込まれたBiosの機能の一つでOSの機能ではない。WindowsなどのOSがスタートする前に、システムそれ自体がパスワードで保護されるのでパスワードを盗み取るUSBなどが設置されていてもBiosパスワードは盗まれることはない。また、起動順序の先頭をHDDにし、設定を勝手に変更されないようにすることもできる。BitlockerはWindowsVista,7のUltimate Enterpriseにしか搭載されていないので一般の個人ユーザーには使用するのが難しいということを考えれば、TrueCryptを使用し、何重にも設定をすることで同等のセキュリティ能力を持つことができるだろう。[13][14]

3.3　提案モデル

ここからは、提案する仮想化暗号化モデルを使用し有効性を評価する。



実線矢印はウィルスが攻撃できる

破線矢印はウィルスが攻撃できない

図 3.1　提案モデル

使用環境

・ホスト PC…Windows XPsp3

・仮想 PC…Windows XPsp3

・使用した仮想ソフト…VirtualBox

・使用した暗号化ソフト…EFS、TrueCrypt

ホストPCでは二つの仮想PCの管理のみを行い、普段インターネットや書類作成など個人情報を含まない作業をする際などは私用仮想PCを使用し個人情報を扱う書類作成や管理は業務用仮想PCを使用しインターネットは切断させておき、2つの仮想PCを完全に独立させる。もしも私用（もしくは、個人情報を扱わないその他の業務) の仮想PCを使用し、インターネットやソフトウェアをダウンロードしウィルスに感染したとしても私用のメモリやディスクは攻撃されるがホストPCや業務用仮想ＰＣのメモリ、ディスクを攻撃されることはない。また、PCを外に持ち出し紛失した場合でも業務用の仮想PCのディスクを暗号化することにより個人情報の流出を防ぐことが出来る。

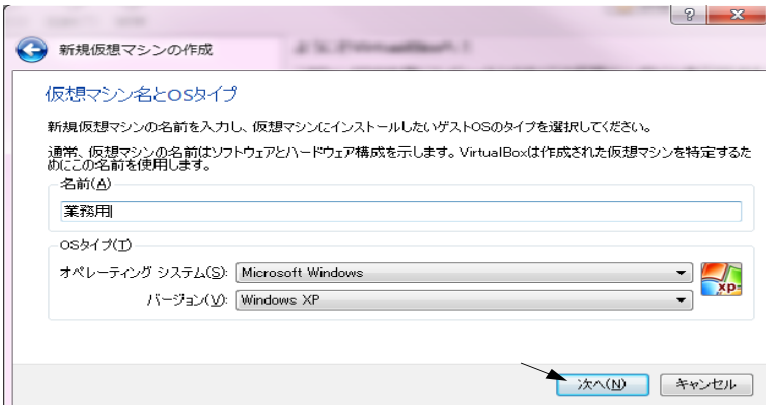
3.3.1　使用した仮想化ソフト、暗号化ソフトの設定

- **VirtualBox**

  VirtualBox インストール後

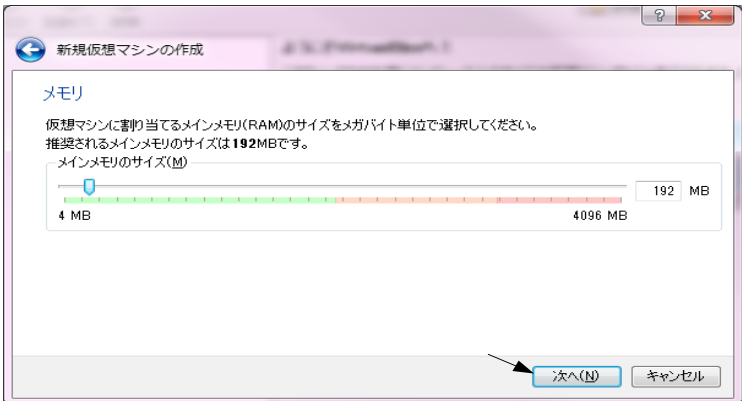
VirtualBox を開き新規をクリック

図 3.2　VirtualBox の設定 (1)



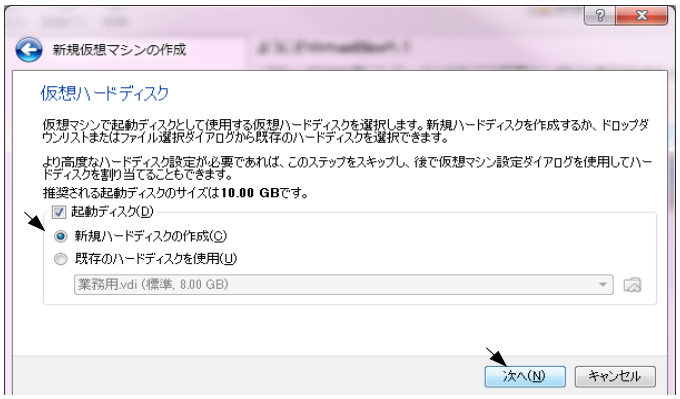
仮想 PC の名前を入力し、使用したいＯＳ、バージョンを設定 → 次へ

図 3.3　VirtualBox の設定 (2)



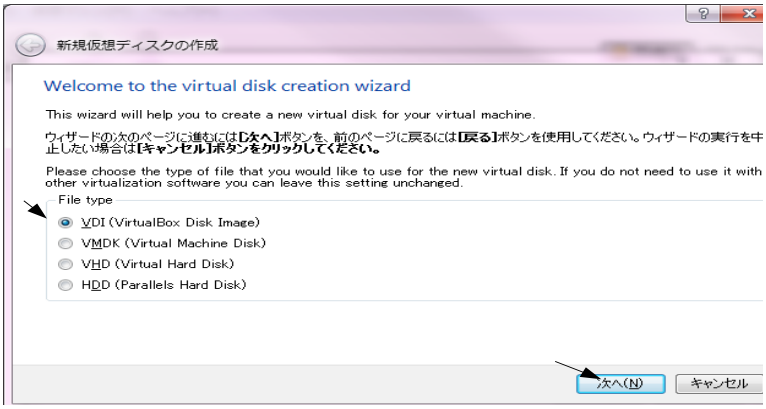
仮想 PC のメモリサイズは変更しない → 次へ

図 3.4 VirtualBox の設定 (3)



新規ハードディスク作成にチェック → 次へ

図 3.5 VirtualBox の設定 (4)

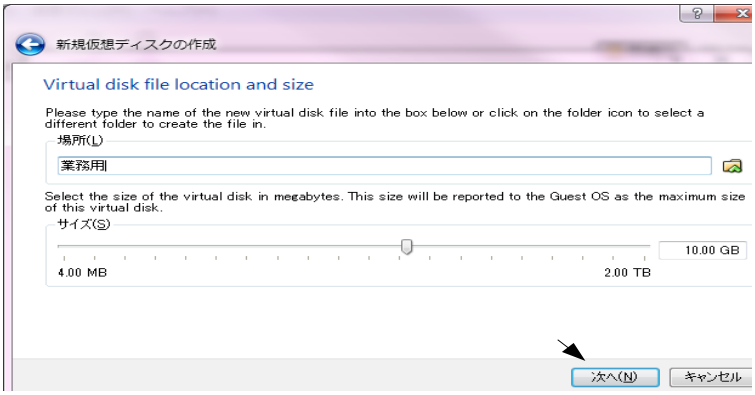


VDI にチェック → 次へ

図 3.6　VirtualBox の設定 (5)

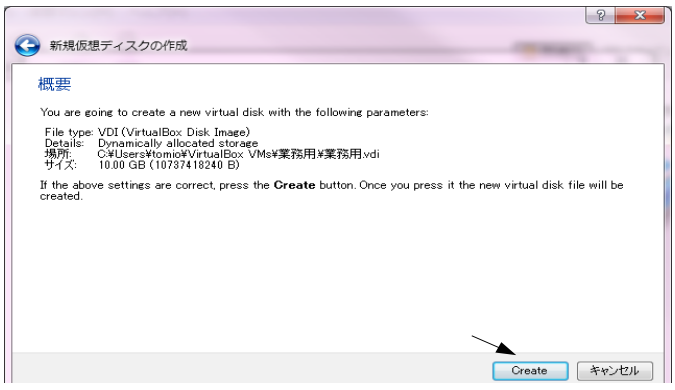
可変サイズのイメージにチェック → 次へ

図 3.7　VirtualBox の設定 (6)



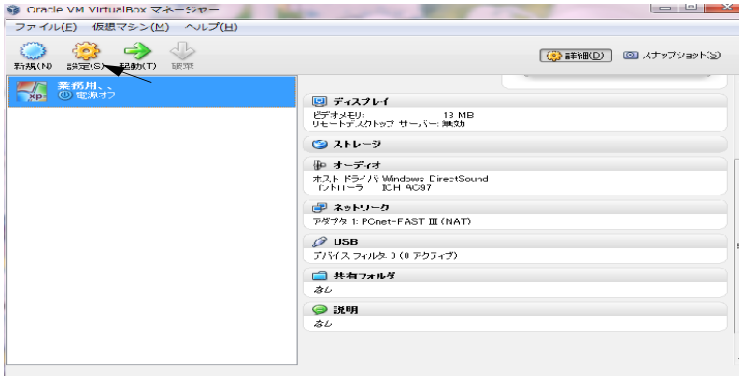
保存先と仮想 PC のサイズは変更しない → 次へ

図 3.8 VirtualBox の設定 (7)



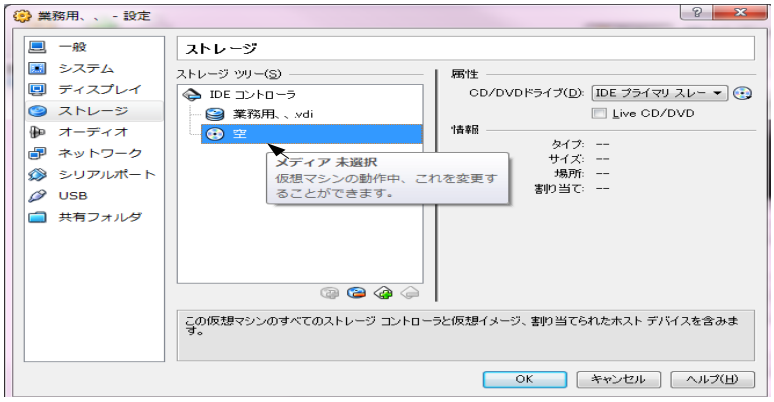
create をクリックし作成完了

図 3.9 VirtualBox の設定 (8)



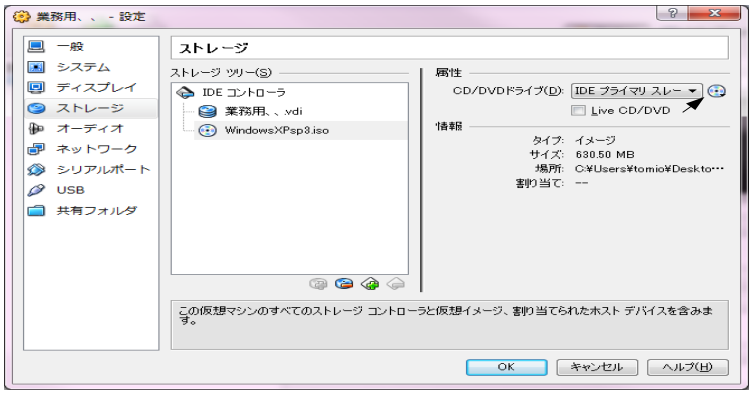
作成された仮想 PC の設定をクリック

図 3.10　VirtualBox の設定 (9)



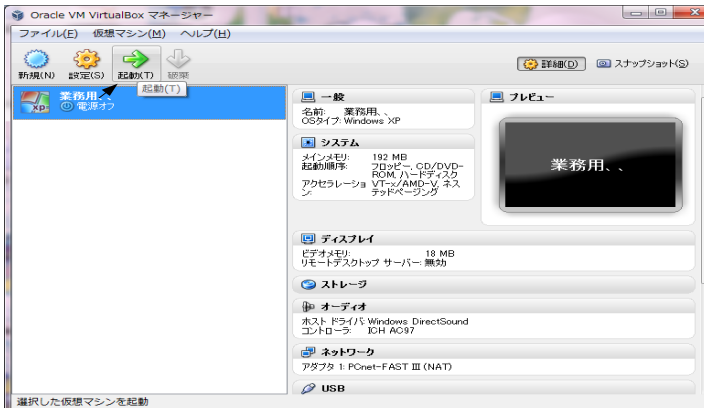
ストレージ → 空をクリック

図 3.11　VirtualBox の設定 (10)



CD/DVD ドライブのアイコンをクリックし OS の ISO イメージを選択

図 3.12 VirtualBox の設定 (11)

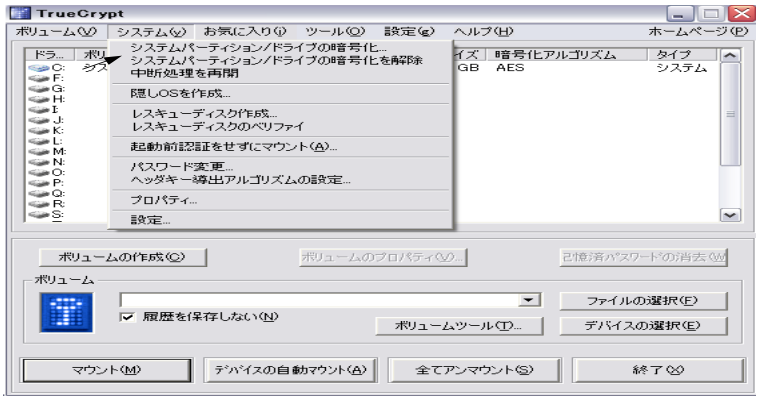


設定完了。起動をクリック

図 3.13 VirtualBox の設定 (12)

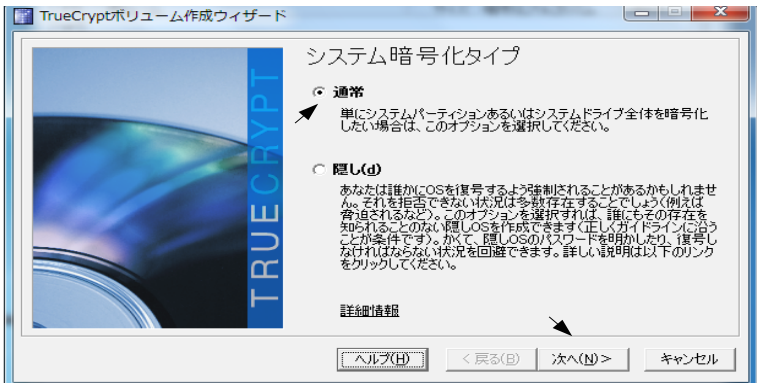
- **TrueCrypt**

  TrueCrypt インストール後



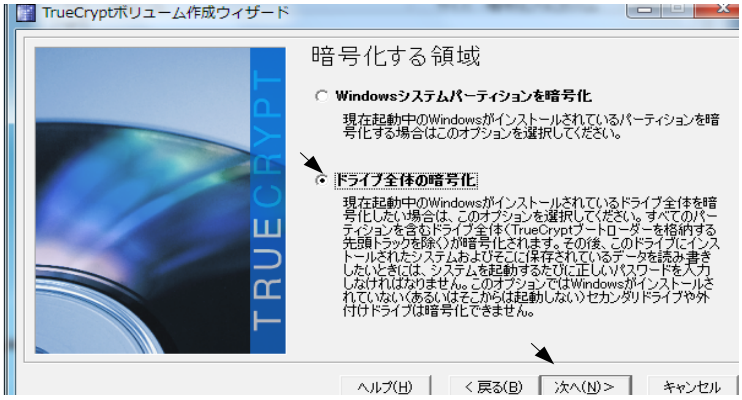
TrueCrypt を開く → システム→システムパーテンション/ドライブの暗号化

図 3.14　TrueCrypt の設定 (1)



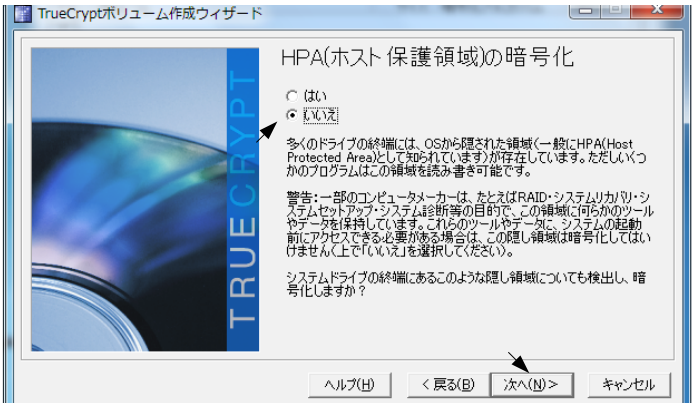
通常にチェック → 次へ

図 3.15　TrueCrypt の設定 (2)



ドライブ全体の暗号化にチェック → 次へ

図 3.16 TrueCrypt の設定 (3)

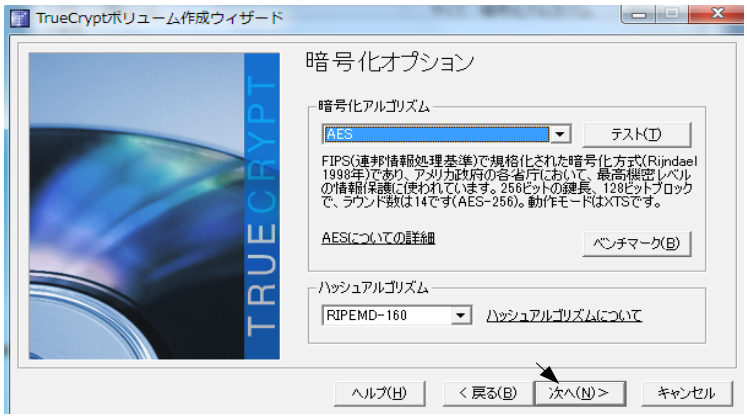


いいえにチェック → 次へ

図 3.17 TrueCrypt の設定 (4)

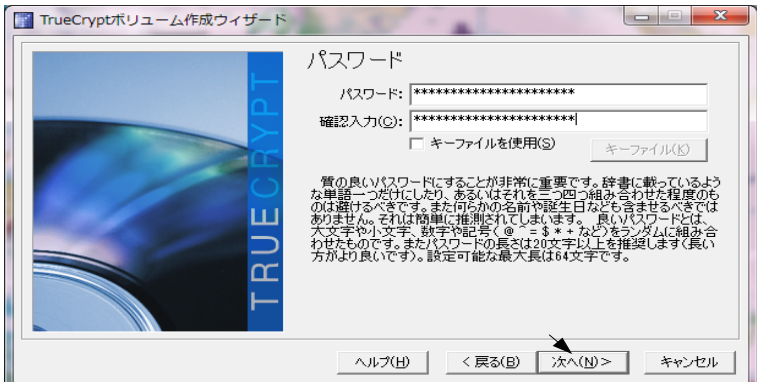
シングルブートにチェック → 次へ

図 3.18　TrueCrypt の設定 (5)



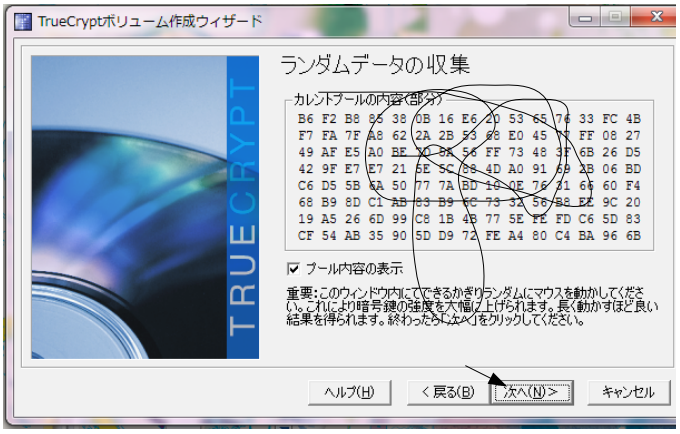
暗号化オプションは変更しない → 次へ

図 3.19　TrueCrypt の設定 (6)



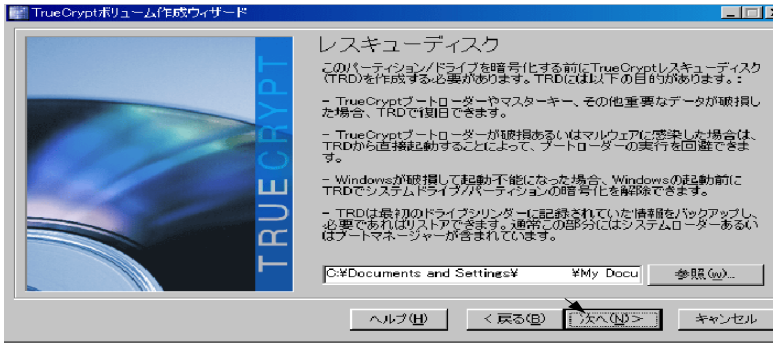
パスワードを入力 → 次へ

図 3.20 TrueCrypt の設定 (7)



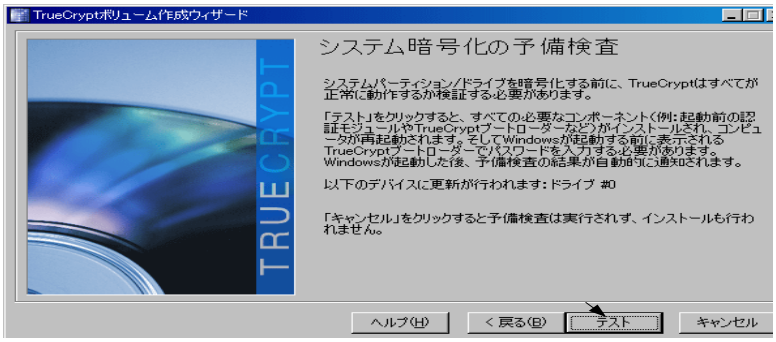
ランダムデータの収集でマウスを無造作に動かす → 次へ

図 3.21 TrueCrypt の設定 (8)



レスキューディスクが作成されるのでディスクにイメージを焼く → 次へ

図 3.22　TrueCrypt の設定 (9)



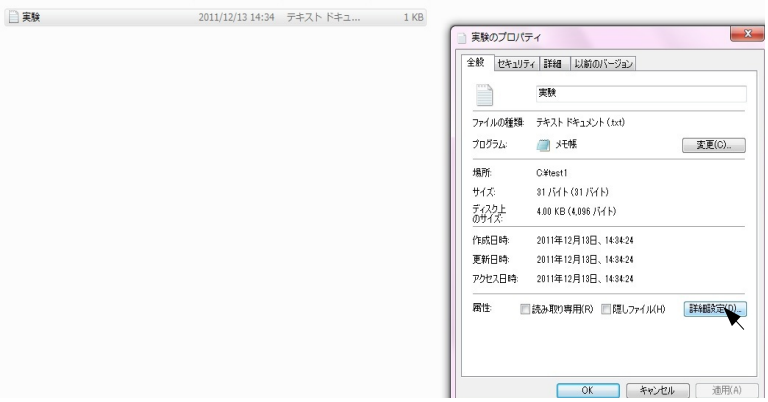
レスキューディスクの認証　→　予備検査 → テスト

図 3.23　TrueCrypt の設定 (10)

テスト後再起動し設定終了

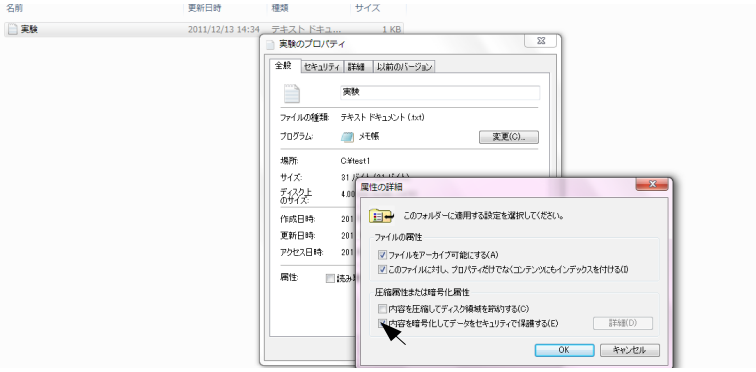
- **EFS**

  ソフトのンストールなどは不要



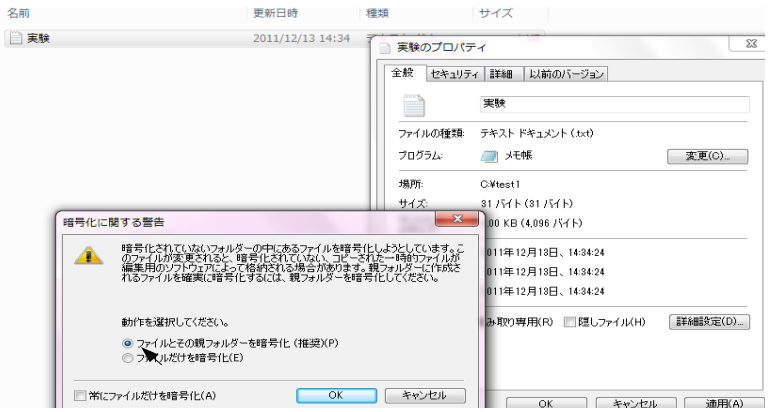
EFS で暗号化したいファイル上で右クリック → プロパティ → 詳細設定

図 3.24 EFS の設定 (1)



内容を暗号化してデータをセキュリティで保護するにチェック → OK

図 3.25 EFS の設定 (2)



適用 → ファイルとその親フォルダーを暗号化にチェック → OK

図 3.26　EFS の設定 (3)

ファイル名が緑色になれば設定は完了

図 3.27　EFS の設定 (4)

3.3.2 提案モデルの実装と実験

使用環境の仮想化、暗号化ソフトを3.3.1の様に設定し実装した。

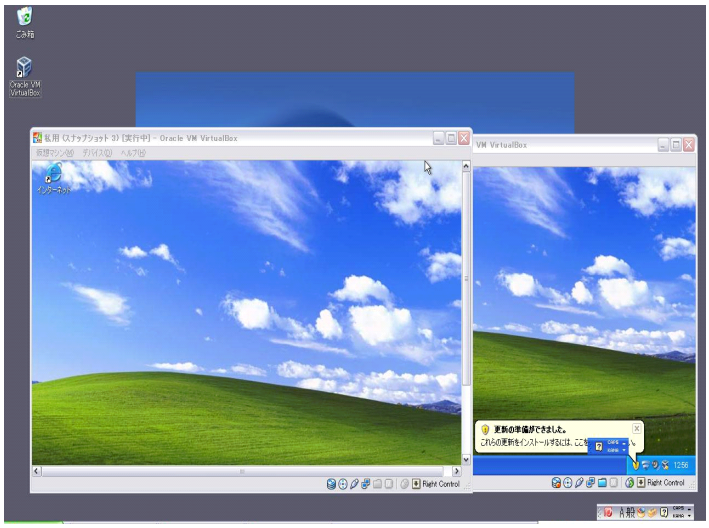


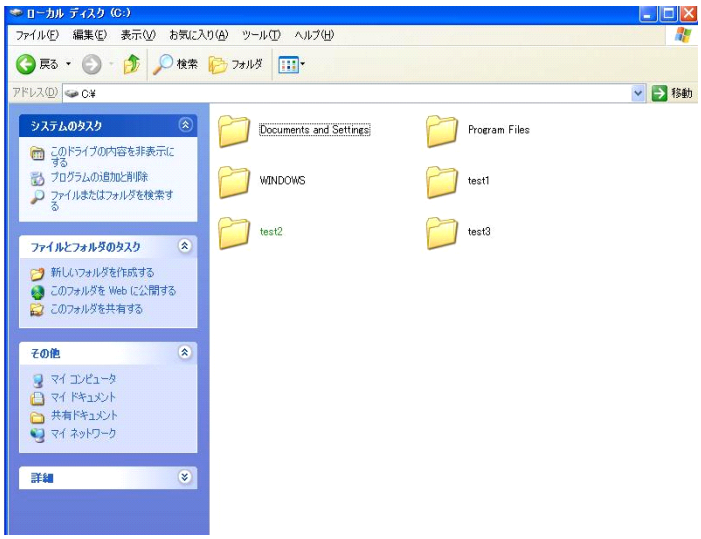
図 3.28 提案モデルの実装

このモデルを評価するために次の2つの実験を行った。

「1」業務用の仮想PC上で作成したファイルをEFSで暗号化し、業務用の仮想ハードドライブを私用の仮想PCにマウントする。業務用で作成した暗号化ファイルを私用の仮想PC上で展開することができるか確認。

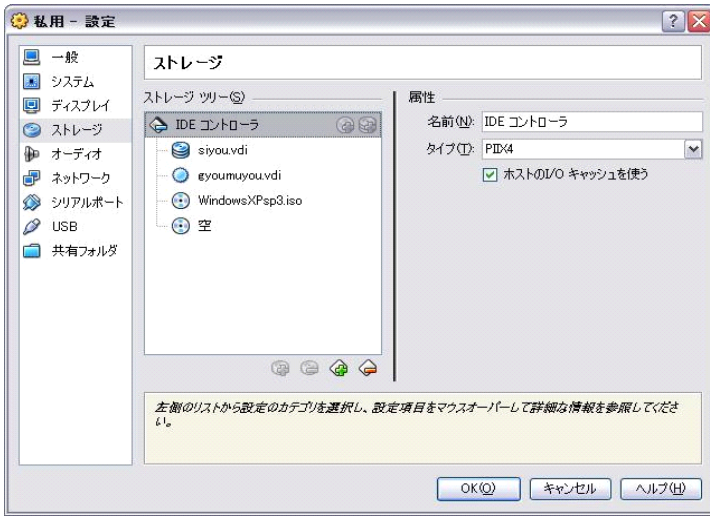
「2」業務用の仮想PCのドライブ全体をTrue Cryptで暗号化し「1」実験と同様の手順で私用の仮想PCにマウントし、私用の仮想PCで展開することができるか確認。

「1」実験



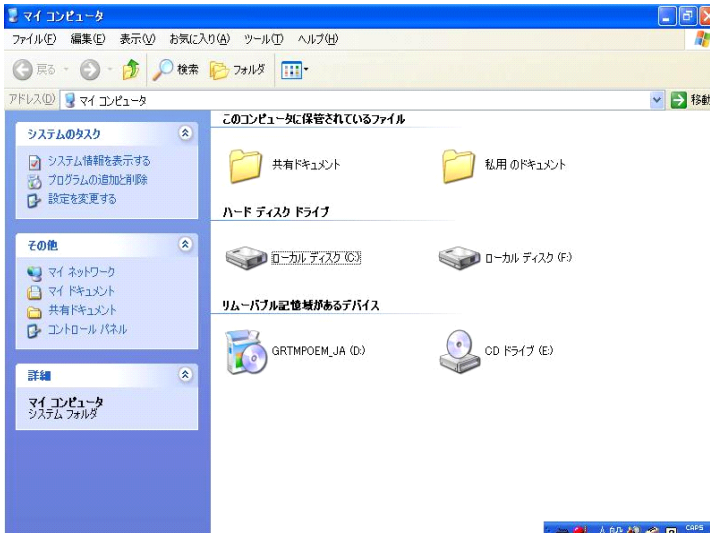
業務用仮想 PC に EFS で暗号化したファイル作成

図 3.29　EFS での実験 (1)



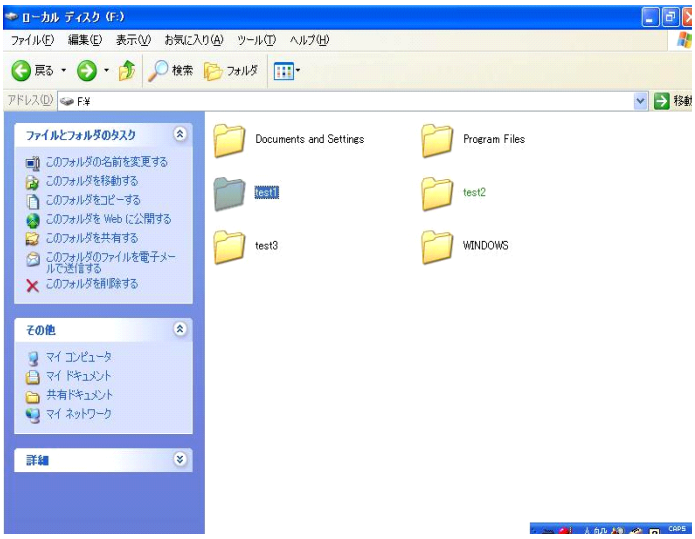
私用仮想 PC に業務用 PC のドライブをマウント

図 3.30 EFS での実験 (2)



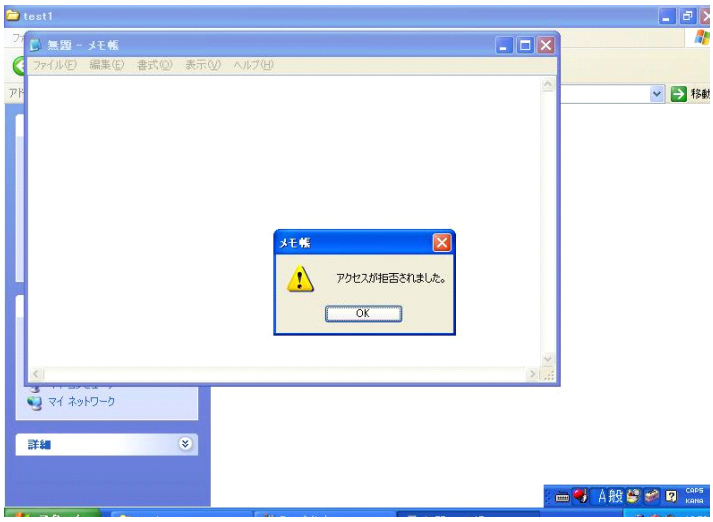
私用のローカルディスク (C) 業務用のローカルディスク (F)

図 3.31 EFS での実験 (3)



業務用のローカルディスク (F) のファイルを開いてみる

図 3.32　EFS での実験 (4)

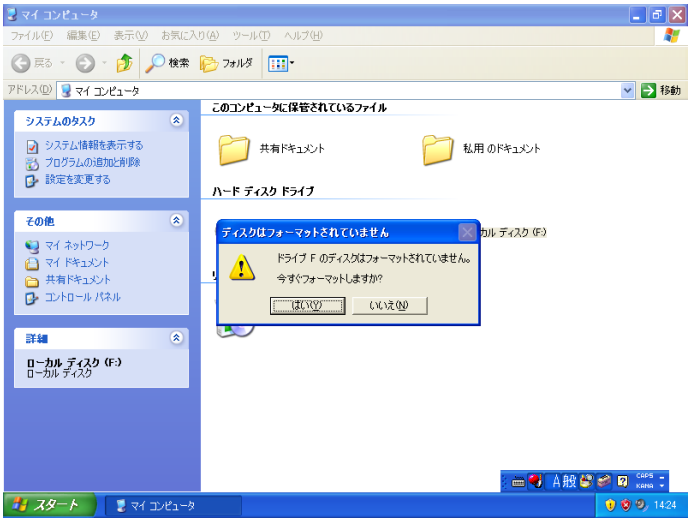


「アクセスが拒否されました」と警告が出て内容を見ることはできなかった。

図 3.33　EFS での実験 (5)

「2」実験

業務用の仮想 PC を TrueCrypt を用いてドライブ全体を暗号化しておき「1」実験の図 3.30〜図 3.32(EFS での実験 (2)〜(4)) と同じ操作を行った。



業務用の「ドライブ F はフォーマットされていません」と警告が出た。
開くためにはフォーマットしなければ内容をみることはできなかった。

図 3.34 EFS での実験 (5)

3.3.3 提案モデルの評価

「1」実験より業務用の仮想PC内でEFSを用いて暗号化したファイルは,、私用の仮想PCではアクセス権が違うため開くことはできなかった。しかし、EFSで暗号化されていないファイルは閲覧可能であった。

「2」実験では業務用の仮想PCのドライブ全体を暗号化し私用PCで開くとフォーマットを要求された。この結果、内部の情報は開くとフォーマットされすべてが消えてしまい個人情報の流出は防ぐことが出来る。

これより提案モデルを実装したパソコンを持ち歩き万が一紛失したときであってもTrueCryptでは情報を閲覧しようと私用の仮想PCに業務用のドライブをマウントしてもまったく情報を閲覧することはできないが、EFSは暗号化されていないファイルは閲覧可能になってしまい安全性に欠ける結果となった。より安全性を高めるのであればファイル単体であるよりも全体を暗号化しておけば1つの情報も外部に漏れ出すことはない。

3.4 まとめ

暗号化ソフトはフォルダーやファイル単体のみを行うものとドライブ全体を暗号化できるものがあるが、単体の場合暗号化するのを忘れたり、ユーザーパスワードを設定していないとまったく意味のないものになってしまう恐れがある。セキュリティーの強度を高めるためにはドライブ全体を暗号化しBiosパスワードを設定するなど多重に防御策を立てておくことである。

提案モデルはウィルス感染と紛失したとき両方に強い環境である。
紛失した場合は、実験で行った様に暗号化されている情報は閲覧することは不可能である。仮想化技術を用いて1つのストレージを分割しているがそれらの仮想PC同士が完全に独立していることが今回の実験でも確認できた。これにより、今回は実験はできなかったウィルス感染においても同様である。万が一私用仮想PCがウィルス感染しても業務用の仮想PCに感染することはほぼないと考えられる。

第4章

SSDのセキュリティについて

4.1 SSDとは

SSDとは、正式名称はSolid State Driveで、記憶媒体としてフラッシュメモリーを利用する記憶装置。ハードディスクの代替として使用できる。

SSDはハードディスクのようにディスクを持たないため、読み取り装置をディスク上で移動させる時間や、目的のデータが読み取り装置の位置まで回転してくるまでの待ち時間が少なく、高速に読み書きできる。また、モーターが無いため消費電力も少なく、機械的に駆動する部品が無いため衝撃にも強いのが特徴である。しかしフラッシュメモリーを利用するので書き換え回数に限度がある。

SSDには2種類あり

・SLC（single level cell）記憶の際ON、OFFの信号しか送らず１つのセルで１ bitの記録を行う。書き換え回数限度10万回
読み込み速度が速いが価格はMLCに比べ高い。

・MLC（multi level cell）記録の際00、01、10、11の4つの信号を使い1つのセルに2bitの記録を行う。書き換え回数限度1万回
読み込み速度が遅く書き換え回数限度もSLCに比べ少ない。[26]

4.2　ウェアレベリングとは

書き換え回数が限られている SSD は使用寿命を延ばすためにウェアレベリングと言う機能が備わっている。書き換えが特定のブロックに集中せず、各メモリセルになるべく均等に分散されるように制御する。この機能は書き込みのときに働く。

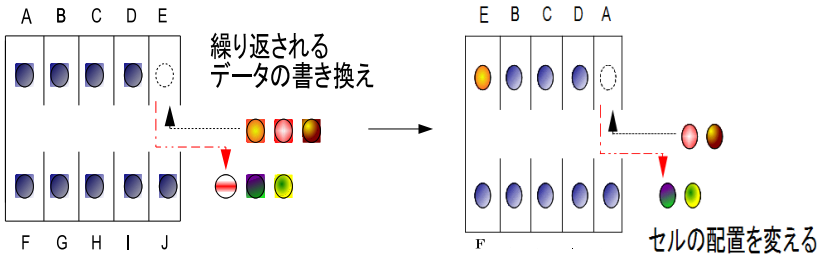


図 4.1　ウェアレベリング

同じ部屋（セル）に何度もデータを書き換えていると限度回数を超え壊れてしまう。そこでウェアレベリングは同じ部屋に何度も書き換えが行われないようにデータを入れる部屋を換える。[8]

4.3 SSD のデータ消去

データを完全消去するには Disk 全体の上書き、フォーマットによる初期化が考えられる。

上書き処理はデータすべてに上書きをして元のデータを消す方法である。だが SSD の場合はウェアレベリングによって、同一のファイルを上書き処理しても、同じファイルに書き込まれる保証はない。この機能が働く場合、ファイルへの上書き処理は、古いセルにデータ痕跡が残ったまま新しいセルに上書きされることになり、データ消去の意味を成さないことが考えられる。

フォーマットは SSD のコントローラは全てのデータを把握しているが、ユーザーが OS から見たときは全てのデータを見ることが出来ないのでフォーマットしたとしても OS 側から確認できるデータは消えるが、SSD 内すべてのデータは必ずしも初期化ができるわけではない。

これらのことから SSD のデータを完全に消去するにはどうすればいいのか検討する。

4.3.1 海外での研究

カリフォルニア大学コンピュータ科学工学部の研究者らは、SSD のドライブ全体や個別ファイルを安全に抹消するために使われている方法には、さまざまな問題があることを発見した。その 1 つが、一部ドライブのファームウェアにおける抹消用の ATA/SCSI コマンドの実装方法である。研究者らが、12 台の SSD(名称は非公表) のドライブ全体の抹消をテストしたところ、抹消に成功したのは 4 台にとどまった。残りの 8 台のうち 4 台は、データ抹消をサポートしておらず (このうち 3 台はリムーバブル USB ドライブ)、1 台は暗号化されていて、抹消できなかった。残る 3 台が抹消に失敗し、うち 2 台はファームウェアのバグが原因だった。1 台は、抹消に成功したと報告したが、データ・パターンがそのまま残っていて、アクセスできた。

一般的なさまざまな抹消プロトコルを使って SSD から 1 個のファイルを抹消

するテストでは、さらに悪い結果となり、4〜75 %のデータが復元可能だった。USB ドライブでの抹消の失敗が目立ち、0.57〜84.9 %のデータが、依然としてアクセス可能であった。研究者らは、NSA(米国国家安全保障局) の承認を受けた消磁機も試した。これは、フラッシュメモリを搭載する SSD には、この技術は有効ではないことを確認するためであった。予想どおり、消磁機は SSD には全く効果がなかった。根本的な問題は、磁気ドライブとは異なり、SSD はデータを物理ページに保存するが、論理ブロック・アドレス (LBA) から消去することにある。このプロセスは、フラッシュ変換レイヤ (FTL) で管理される。このことから、ATA ドライバや SCSI ドライバが、データが存在すると認識する場所と、データが物理的に存在する場所が食い違ってしまうということになる。SSD はデータをあちこちにコピーすることで、この食い違いを解消している。このコピーのせいで、データの危険な痕跡が SSD 内に散乱していると言える。

SSD ユーザーは、HDD 用の抹消技術を適用すれば、SSD データは基本的に復元できなくなると思い込んでいるかもしれない。実際には、データが SSD 上に残り、少し高度な技術を使うだけで、復元できてしまう可能性があると研究者らは言及している。[8][27]

このアメリカでの研究報告では3つの結論が導き出された。
1. データ消去の技術は、製造メーカによってしばしば実装されることがあるが、効果的でない。
2.SSD のOSから見えるアドレス空間全てに複数回上書きすることは普通であるが、それがドライブ内のデータを全てを消去するには不十分である。
3. 既存のHDD に適した技術は、SSD の個々のセル内の情報を完全に消去するのにはどれも効果的ではない。

3. 結論より、SSD はデータを物理ページに保存するが、データの消去は論理ブロック・アドレス(LBA) から行うというプロセスはフラッシュ変換レイ(FTL) で行われ、この機能を改良することによりSSD 内蔵のフォーマットオペレーションになると結論付けている。[27]

しかしこれはまだ研究段階であり根本的な解決方法ではない。

4.4 まとめ

今まで説明してきたことによりSSD のデータを完全に削除することは不可能という結論に至った。

私たちができる最低限のことは、SSD を使用する前にディスク全体を暗号化することである。ドライブを暗号化してから使い始めれば、暗号化キーを削除することで、フルドライブを消去できる。[10]

SSD はHDD に比べ衝撃に強い、消費電力が少ない、動作音が無い,、低温時・高温時の作動も安定し故障に強い、データ読み込みが早い、軽いとメリットが多い。しかしSSD 内臓のPC を買い替えたり、廃棄するのは全てのデータを消せないので危険である。

第5章

結論

本研究では暗号化ソフトの有効性の評価、提案モデルの実証、SSD の廃棄時のデータ消去について述べてきた。

暗号化ソフトについてEFS はフォルダやファイルのみを暗号化するのでホストユーザ-はログインパスワード、休止状態からの復帰の際にもパスワードを設定しなければ意味がなくなってしまう。これは、EFS は HDD 内に復号化するための秘密鍵が入っているためであり、使用する際には扱い方を考慮する必要がある。TrueCrypt などドライブ全体を暗号化できるものは 20 文字以上のパスワードを設定することで強固なセキュリティになるが、そのパスワードを忘れたり、読み取られたりすると意味がなくなってしまう。暗号化ソフトだけを使用し完全に安全であるという保障はなく、PC を最新版に更新するのを忘れずに行うことと、PC に備わっている Bios パスワードやログインパスワードを使用することにより安全度は向上する。

提案モデルは仮想 PC 同士が完全に独立しているため物理的な攻撃にもウィルス感染にも有効なモデルであると考えられる。またメモリついても同様である。、OS 上でプログラムを起動すると、OS がプログラムを実行・管理する単位としてのプロセスが生成される。OS 上で生成されたプロセスには、仮想アドレス空間が割り当てられ、それぞれのプロセスは独立したものである。あ

るプロセスから別のプロセスの仮想アドレス空間にアクセスすることはできない。よってウィルス感染した私用の仮想PCのメモリから業務用の仮想PCのメモリに感染することはほぼないと考えられる。しかし、これはまだ研究段階でありこのモデルにセキュリティホールがないかなどを今後の研究で試してもらいたい。[17][19][20][21]

SSDはフラッシュメモリであるので書き込み回数制限がある。そのため、使用寿命を延ばすためにウェアレベリングという機能が備わっている。
しかしこの機能が逆にSSDなどのフラッシュメモリの機器のデータ消去を難しくしている。既存のデータ消去などはほとんど効果的ではなく今現在SSDを完全に消去するソフトは存在しない。データを破棄したい場合は使い始める前にSSD全体を暗号化し消去するときは暗号化キーを削除することで、全てのドライブを消去する以外方法がない。

この先ますます私たちはモバイル機器を使用していく機会が増えていく。そのためどんな危険性があり、どのような対処法があるのかを頭の片隅に置きモバイル機器に存在する個人情報の安全を守っていかなければならない。そのために本研究はセキュリティ対策のマニュアルを作成するための一部を研究、評価した。今後モバイル機器の考えられる全ての危険性を評価、検討しマニュアルを完成することを願っている。

謝辞

本研究を行うにあたり、終始熱心に御指導していただいた木下 宏揚教授に心から感謝致します。また、研究活動一般に様々な助言を頂きました南出和宏氏をはじめ公私にわたり良き研究生活を送らせていただいた木下研究室の方々に感謝致します。

2012 年 2 月
田中　友之

参考文献

[1] 中村真彦：”仮想化技術パーフェクトガイド”，ソーテック社, (2007)

[2] 平 初, 宮原 徹, 伊藤　宏通, 野津　新, 鎌滝　雅久, 中村　正澄, 宮本久仁男, 小野　雄太郎, 大島孝子：”仮想化技術完全攻略ガイド”，インプレスジャパン, (2006)

[3] 若林　宏 :”よくわかる最新暗号技術の基本と仕組み :” 暗号と暗号化方式の基礎を学ぶ : 暗号の常識”, 秀和システム, (2005)

[4] 島崎聡史, 吉田佳宏, ビーナス・テクノロジィズ :”仮想化技術徹底活用 : サーバ管理者/システム開発者のための,”秀和システム (2008)

[5] 橋本和則 :”PC 仮想化テクニック : 1 台で Vista も XP もスッキリ使い分け”, 翔泳社, (2007)

[6] 清野克行 :”仮想化の基本と技術 : 仕組みが見えるゼロからわかる : Information Technology”, 翔泳社, (2011)

[7] 北嶋伸安 :” Oracle VM サーバー仮想化構築ガイド”, アスキー・メディアワークス,(2008)

[8] ”SSD のウェアレベリングのしくみ”
http://www.pc-info.sakura.ne.jp/ssd-wea.html

[9] ”HDD 用データ抹消技術ではSSD データの抹消は困難ー米研究者が報告”
http://www.computerworld.jp/topics/561/ストレージ/190777/HDD 用データ抹消技術ではSSD データの抹消は困難

[10] ”SSD のデータを安全に消去したければ使用前にドライブを暗号化するべし”
http://www.lifehacker.jp/2011/03/110225ssddelete.html

[11] ”Microsoft”
http://windows.microsoft.com/ja-JP/windows7/Whats-the-difference-between-BitLocker-Drive-Encryption-and-Encrypting-File-System

[12] ”Windows XP Professional のスタンドアロン環境 で暗号化ファイルシステムを使う場合の注意点”
http://07.net/EFS/

[13] ”TrueCrypt に対する Evil Maid 攻撃に関する検証レポート”
http://security.intellilink.co.jp/article/vulner/pdf/report20091109.pdf

[14] ”Ken’s Memo”
http://kenmemo.blogspot.com/2010/11/tpm.html

[15] ”ボリューム・レベルの暗号化機能「Bitlocker」の仕組みを知る ”
http://itpro.nikkeibp.co.jp/article/COLUMN/20070611/274342/

[16] ”ストレージを守るセキュリティ技術”
http://ascii.jp/elem/000/000/480/480085/index-2.html

[17] ”他プロセス・メモリの Read、Write について”
http://social.msdn.microsoft.com/Forums/ja/vcgeneralja/thread/caa5b07e-52b8-43fd-99af-7bcef325d6f3

[18] ”Windows セキュリティ・ワンポイントレッスン”
http://www.st.rim.or.jp/ shio/winsec/hibernation/

[19] ”ホワイトハッカー道場”
http://itpro.nikkeibp.co.jp/article/COLUMN/20070927/283156/

[20] ”Interstage Application Server/Interstage Web Server チューニングガイド ”
http://software.fujitsu.com/jp/manual/manualfiles/M080099/J2UZ9570/03Z2A/tun07/tun0

[21] ”プロセスとメモリ”
http://www.doppo1.net/os/memory.html

[22] ”九州大学・情報漏洩対策マニュアル”
http://www.cc.kyushu-u.ac.jp/ec/guidance/security-manual/

[23] ”法的技術今日”
http://www.legaltechtoday.com/ja/2011/03/31/ssd-security-the-worst-of-all-worlds-zdnet/

[24] ”ファイルやフォルダを簡単に暗号化する「TrueCrypt」 ”
http://itpro.nikkeibp.co.jp/article/COLUMN/20081117/319367/

[25] ”テンポラリファイルから情報が漏れる ”
http://www.ipa.go.jp/security/awareness/vendor/programmingv1/b07_08.html

[26] ”IT 用語辞典”
http://e-words.jp/

[27] Michael Wei, Laura M. Grupp, Frederick E. Spada, Steven Swanson Department of Computer Science and Engineering, University of California, San Diego Center for Magnetic Recording and Research, University of California, San Diego:Reliably Erasing Data From Flash-Based Solid State Drives:(2011)

[28] ”VirtualBox の使い方”
http://virtual-soft1.nnn2.com/

[29] ”パスワード対策　破られにくいパスワードの作り方と盗用予防”
http://enchanting.cside.com/security/password.html

[30] ”Vistaで導入された電源制御「スリープモード」とは？”
http://stakasaki.at.webry.info/200703/article_4.html

[31] ”FireWire経由でWindowsログインパスワードを迂回するツール”
http://japanese.engadget.com/2008/03/04/firewire-windows/

[32] ”Windowsにおけるバッファオーバーフロー”
http://www.st.rim.or.jp/ shio/csm/winbof/

質疑応答

豊島先生より

Q：

松澤先生より

Q：