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

木下研究室　　田中　友之 (200803001)

1　はじめに

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、こういった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、情報漏洩の防止対策に役立てること、特に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洩の対策を検討しその安全を評価することを目的とする。

2　仮想化と暗号化

2.1　仮想化

仮想化とは、コンピューターシステムにおける物理ソースの抽象化である。

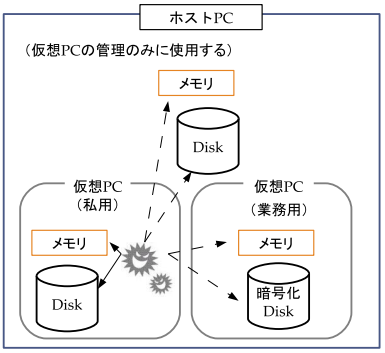
仮想化のメリットとして
(1) パーティショニング＝1つのストレージを分割し, 同時に複数の仮想 PC を実行できる
(2) 隔離＝同じハードウェア上の仮想 PC 同士を完全に独立状態で稼働できる
(3) カプセル化＝ハードウェア構成、Bios, ディスクの状態など仮想 PC 全体を物理ハードウェアから独立したファイルに保存できる。
この３点が挙げられる。

2.2　暗号化

暗号化とは重要な情報の入ったノート 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が必要である。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。

暗号化ソフトには個々のファイルやフォルダーだけを暗号化するものとディスク全体を暗号化するものがあるが、より安全性を高めるのであれが全体を暗号化した方が良い。

2.3　提案する仮想化暗号化モデル



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 1: 提案モデル

ホスト PC では二つの仮想 PC の管理のみを行い、仮想 PC は私用、業務用と独立させる。もし、紛失した場合に備えて業務用のディスクを暗号化する。

このモデルでは、ウィルス感染、紛失による情報漏洩を防ぐことが出来る。

2.4　提案モデルでの実験

このモデルを評価するために以下の実験を行った。

(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。結果、私用の仮想 PC で業務用の暗号化ファイルを開くことが出来なかった。

(2) 業務用の仮想 PC のドライブ全体を True Crypt で暗号化し (1) 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。結果、私用の仮想 PC で業務用のドライブを開こうとするとフォーマットしなければ開くことができなかった。

3　まとめ

この実験結果より仮想化は1つのストレージを分割し、複数の仮想 PC を実行しているが、それらの仮想 PC 同士が完全に独立していることがわかる。

これより、私用の仮想 PC で万が一ウィルス感染した場合でも業務用の仮想 PC に被害が及ぶことはないと考えられる。