O-026

使用目的を限定したソフトウェア仮想化環境のためのセキュアな USB メモリの活用
Secure Utilization of USB Flash Drive for Limited Software Platform Virtualization

髙橋 雅隆† 納富 一宏†
Masataka Takahashi Kazuhiro Notomi

1. はじめに

パソコンは，その使用目的の多様化により，現代社会では企業だけでなく大学や高等学校などを含む教育機関や一般的な家庭にまで広く普及している．現在では，利用場所に依存することのない環境の整備が，ネットブックやスマートフォンなどを含むモバイル機器の普及とクラウドコンピューティング技術や公共交通機関への無線 LAN 導入などを含むユビキタス化の進展により着実に進められている．

しかし，利用者ごとに使い慣れたプラットフォーム（OS）やアプリケーションソフトなどを含むコンピュータ環境の違いから生じる作業効率の低下や作業自体が行えなくなるといった状況が考えられる．市販の製品では，セキュリティ機能付きの USB メモリにコンピュータ環境を構築して持ち運びを可能にするものがあるが，価格が高いため，利用者にとって導入の敷居が高い場合が多い．

本研究では，これらの問題を解決するために暗号化および仮想化を実現するオープンソースソフトウェア（OSS）を利用し，USB メモリ領域内の暗号化を施した仮想ディスク内に仮想化環境を構築する手法によって，安全かつ低コストでコンピュータ環境の持ち運びを可能とするシステムの提案および実装を行ってきた[1]．本稿では，本手法の実用化および使い勝手の向上を目的とし，特定のアプリケーションソフト利用に限定した場合のシステムの改善について検討を行う．

2. 環境可搬システム

2.1 システム構築に利用した OSS

本研究では，コンピュータ環境の持ち運びを可能とするシステム構築において，特定のパソコンへの依存がなく，USB メモリでの持ち運びが可能な OSS を使用している．

2.1.1 仮想化ソフトウェア

仮想化ソフトウェアとは，図 1 のように OS 上で別の OS を動作させるためにハードウェア層をエミュレートした仮想マシンを作成し，仮想マシン内で OS を動作させるソフトウェアのことである．

図 1 アプリケーション型の構成

仮想化ソフトウェアには，ハイパーバイザー型，パーティショニング型，アプリケーション型があり，本研究では，ホスト OS 上での動作が可能であるアプリケーション型の Portable-VirtualBox 4.0.4 を使用している．

† 神奈川工科大学大学院工学研究科 Graduate School of Engineering, Kanagawa Institute of Technology

2.1.2 暗号化ソフトウェア

暗号化ソフトウェアとは，パソコン内に保存されているデータファイルを盗難や不正利用から守るためにハードディスクを含む記憶媒体やデータファイルに暗号化を施すソフトウェアのことである．本研究では，暗号化を施したデータファイルを OS にハードディスクとして認識させることが可能な TrueCrypt 7.0a Portable Mode を使用している．

2.2 実現方法

本研究では，OS およびアプリケーションソフトなどを含むコンピュータ環境を持ち運ぶことを目的として構築したシステムを「環境可搬システム」，仮想化ソフトウェアで構築した仮想マシン（コンピュータ環境）のことを「仮想化環境」としている．

本システムを実現するにあたり，先述した 2 種類の OSS と Visual C++ .NET 2003 で作成した 2 つのプログラム（モジュール）を組み合わせることでシステムの構築を行った．環境可搬システムの構成を図 2 に，環境可搬システムを構成する OSS や作成したモジュールの詳細を表 1 に示す．

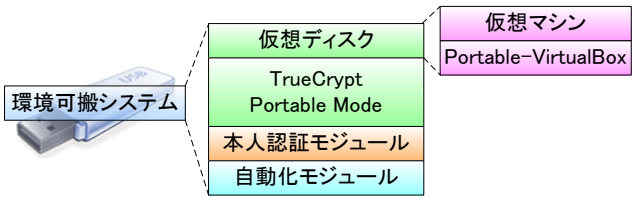

図 2 環境可搬システムの構成

表 1 環境可搬システムの構成要素の詳細

モジュール名	用途
自動化モジュール	パスワード入力以外の手動操作の自動化
本人認証モジュール	パスワード入力による本人認証
TrueCrypt Portable Mode	暗号化処理を施した仮想ディスクの作成（情報流出対策）
仮想ディスク	Portable-VirtualBox および仮想マシンの保存先
Portable-VirtualBox	仮想化環境の構築と実行
仮想マシン	コンピュータ環境を仮想化環境として構築

本システムを構成する上で作成したモジュールの機能を以下に示す．

- 自動化モジュール
  - 本人認証モジュールの実行から仮想化環境の終了までのパスワード入力以外の手動操作の統合および自動化（ソーシャルエンジニアリング的手法の対策）
- 本人認証モジュール
  - 自動化モジュール実行後にパスワード入力による本人認証を実行

➢ OpenSSL[2]（オープンソースライブラリ）のハッシュ関数（ハッシュアルゴリズム：SHA-256）によるパスワードの暗号化および照合

なお，本システムが現段階で正常動作するホスト OS は，Windows XP，Windows 7 である．

2.3 システムの処理過程

USB メモリをパソコンに接続してからの本システムが実行する動作をフローチャートとして図 3 に示す．

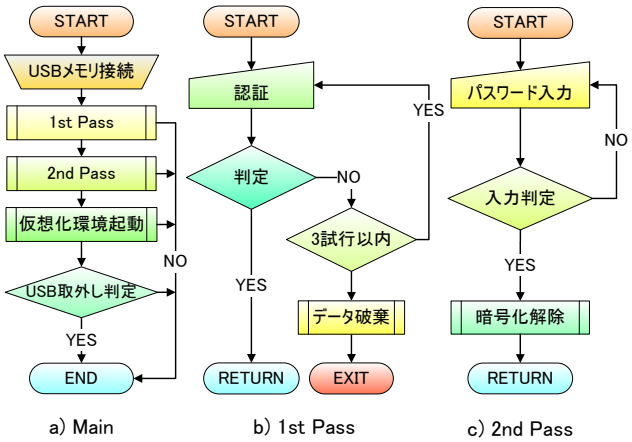

図 3　環境可搬システムが行う処理

本システムは，USB メモリ接続後に自動化モジュールを実行することで，1st Pass である本人認証モジュールを実行する．認証成功の場合，TrueCrypt Portable Mode による仮想ディスクの復号化処理を行う．次に，仮想ディスク内の Portable-VirtualBox を実行し，構築した仮想化環境の起動を行う．最後に，仮想化環境終了後の処理として，USB メモリの取り外し処理を行う．また，1st Pass での認証失敗時の処理として，仮想化環境からの情報流出を防止するために USB メモリのデータ破棄を行う．

なお，従来の 1st Pass による本人認証はパスワード認証のみであったが，現在では，身体的・行動的特徴を用いる生体（バイオメトリクス）認証の実装を行い，パスワード認証との選択・併用が可能となるようシステムの拡張を実現している[3]．

3. 環境可搬システムの実用化

本システムの提案および実装では，本学情報工学科の授業で使用するコンピュータ環境を仮想化環境として構築し，ユーザによる評価実験を行った[1]．実験結果から，使用するアプリケーションソフトによって操作性は左右されるが，仮想化環境でも問題なく作業を行えることを 確認した．本稿では，評価実験の結果を踏まえた上で，本システムの実用化と使い勝手の向上を図る方法の一つとして，使用目的を限定した本システムの利用について着目した．

3.1 システムの改善点

本システムの使い勝手向上を目的として，以下に示す機能や処理をシステムに新規追加した．

（1）本人認証モジュールの選択・変更機能
（2）仮想化環境の自動起動 ON/OFF 機能
（3）ホスト PC のインストール済み OSS の利用
（4）仮想化環境で使用するメモリ容量の自動割り当て
（5）システム終了時における USB メモリ取り外し

これらの機能の追加により，パスワード入力以外の認証モジュールの利用（1）やシステム実行以降に使用したい仮想化環境の選択（2）が可能となる．また，使用するホスト PC に合わせた最適なメモリ容量の割り当て（4）や USB メモリの取り外しの自動化（5）により，システムで行う操作の円滑化が可能となる．特に TrueCrypt と VirtualBox がホスト PC に存在する場合における競合状態の回避処理（3）を行うことにより，仮想化環境が起動できなくなる不具合を解消した．

3.2 使用目的を限定した仮想化環境の構築

本稿で提案する仮想化環境は，提案・実装時に構築した多目的利用を想定した仮想化環境とは異なり，文章作成やプレゼンテーションツールの利用，プログラム開発などといった使用する目的を限定する．これにより，OS の起動後に使用目的に合致したアプリケーションソフトの自動実行が可能となり，作業に着手する上で必要な操作であるアプリケーションソフトの選択・実行を簡略化することが可能になる．また，Portable-VirtualBox の機能の一つである仮想マシンの状態保存機能を利用して，OS 起動後の状態を保存することによって，作業着手までにかかる時間を短縮することも可能である．ただし，この機能を利用するには，あらかじめ仮想化環境の起動を行う必要がある．

3.3 考察

システムの改善を行った結果，システムに新規追加した機能や処理によって，システムの実行から USB メモリの取り外しまでに行う一連の操作が円滑に行うことが可能になった．また，使用目的を限定した仮想化環境の構築によって，仮想化環境の OS 起動後から作業着手までに必要な操作手順を簡略化することが可能になった．これらのことから，初期システムよりも手動操作を減らすことによって，安全性と使いやすさが向上すると考えられる．

4. おわりに

本稿では，環境可搬システムの実用化および使い勝手の向上を踏まえたシステムの改善について述べた．

環境可搬システムの改善として，システムに新規追加した機能や処理によって，初期システムよりも全体的に操作をよりスムーズに行うことが可能となった． また，仮想化環境の使用目的を限定したことによって，OS 起動後のアプリケーションソフトの自動実行が可能となり，作業着手までの手順を簡略化することが可能になった．今後，本システムを実用化する上で手動操作のさらなる簡略化を行う予定である．

参考文献

[1] 高橋雅隆，中山亮介，納富一宏，“セキュリティを考慮した仮想化環境による USB メモリの活用”，2010 年度画像電子学会第 38 回年次大会 S4-3(2010.06).
[2] John Viega，Matt Messier，Pravir Chandra(共著)，齋藤孝道(監訳)，“OpenSSL－暗号・PKI・SSL/TLS ライブラリの詳細－”，pp.26-28，pp.225-232，株式会社オーム社(2004).
[3] 高橋雅隆，山内俊明，納富一宏，斎藤恵一，“自己組織化マップを用いた顔画像による個人識別”，電子情報通信学会，2010 年度 HCG シンポジウム B2-3(2010.12).