# 修 士 論 文 の 和 文 要 旨

| | | | |
|---|---|---|---|
| 研究科・専攻 | 大学院　電気通信学研究科　情報工学専攻　博士前期課程 | | |
| 氏　　名 | TRAN TRUONG DUC GIANG | 学籍番号 | 0931033 |
| 論 文 題 目 | 準パススルー型仮想マシンモニタへのマルウェア検出機能の拡張 | | |

要　　旨

仮想マシンモニタ（VMM）を用いたセキュリティ向上は，最近数年の間に非常に良く研究された効果的なアプローチである. BitVisor はストレージデータの暗号化や VPN の構築を含む多様なセキュリティ機能を提供する VMM である．BitVisor は準パススルー型アーキテクチャを用いて構築されている．そのアーキテクチャでは，OS からの大半の I/O アクセスは VMM を通過し，セキュリティ機能を実装するための最小限のアクセスだけが VMM によって捕捉される．そのアーキテクチャは小さいオーバヘッドと Trusted Computing Base（TCB）をもたらす．現在の BitVisor はプライバシーの保護はできるが，マルウェアの検出はできない．そこで本研究では，マルウェア検出機能を準パススルー型 VMM に組み込むための方式を提案する．我々はその方式に基づいて BitVisor の拡張を実装した．その拡張は，データ I/O の中身を，VMM に保存されたマルウェアのシグネチャと比較する．我々は実験を行い，その拡張が Linux と Windows などの OS に関係なく，実在のマルウェアを高い精度で検出できること，その拡張の実行時間オーバヘッドが小さいことを確認した.