研究課題別中間評価結果

1． 研究課題名： 耐攻撃性を強化した高度にセキュアな OS の創出

2． 研究代表者： 河野 健二（慶應義塾大学理工学部 准教授）

3． 研究概要

オープンシステムディペンダビリティーを高めるためには、システムのセキュリティ機構は様々な脅威に対処可能な仕組みを備えていなければならない。これまでに認証や認可、アクセス制御などのセキュリティ機構が OS に組み込まれてきた。本研究課題では、仮想化テクノロジー、セキュリティチップなど最新の技術動向を踏まえ、オペレーティングシステム（OS）カーネルそのものの健全性を担保するための要素技術の研究開発および統合を行っている。

本研究は仮想化テクノロジーをベースとして OS のセキュリティ向上を目指して推進している。仮想マシンモニタは OS とは明確なハードウェアインターフェースで分離されており、OS の動作を外部から観察することができる。河野グループでは仮想マシンモニタ層から OS の異常な動作を検知し、マルウェアを検知する技術の研究を進めている。特定の検体に依存することのない汎用的な手法により、ルートキットやキーロガーの検知に成功しており、その技術の一部は同領域の中島チームが開発している仮想マシンモニタに統合済みである。また、光来グループではマルウェアの検知機構を安全に動作させるための基盤技術の研究を進めており、既存のセキュリティソフトウェアに適応できるまでの高いレベルに到達している。さらに、両グループで推し進めてきた OS の健全性回復技術においては、国際的にも高い評価を得ることができている。これらの研究成果により、OS のセキュリティを強化するセキュリティ基盤構築に向けて有益な知見を蓄積しつつある。また、統計的手法を用いたアプリケーション層における障害の早期検知にも取り組んでおり、実ワークロードを模したベンチマークにおいて早期に障害を検知できることを確認済みである。

4． 中間評価結果

4－1. 研究の進捗状況及び研究成果の現状

ディペンダビリティー向上に向けた重要な要素の一つであるセキュリティについて、仮想化機構を用いることによって攻撃の種類に対する個別な対応を超えた汎用的なセキュリティ実現の手法を開発し、中島チームと協力してこれを DEOS 実行環境（D-RE）内に統合実装し、有用性を確認している。具体的には、D-System Monitor と D-Visor を連動させ、監視対象 OS が行う特権レジスタへのアクセスや特権命令の実行、入出力やその内容などを正確に監視することによって通常動作との差異を検出し、キーロガーの検知、ファイルメタデータ改竄ルートキットの検知、ボット検知、ブラウザ寄生型マルウェアの解析、などを実現している。また、より高いセキュリティを確保するための VM の構成法についても具体的な研究成果を上げている。

OS カーネル内のバグによる悪影響に対しては健全性を維持するためには再起動による対応が現実的であるが、通常の再起動には長い時間を要する。本研究チームは高速な障害復旧機能（高速リブート機能）に関する新たな手法（phase- based reboot 並びに warm-cashe reboot）を開発し、国際的に高く評価されている。本手法は DEOS プロセスにおける障害対応サイクルの実現に貢献することが期待されている。さらに、障害の予兆検出に関する研究も進んでおり、全体として予想を上回る大きな成果を上げている。

研究実施体制については、少数精鋭で高い成果を上げている。また、中島チームをはじめとする他の研究チームとの連携もうまくとれていると考える。研究費の執行状況についても適切である。

4－2. 今後の研究に向けて

これまでに非常に高いレベルの成果を出しており、継続してさらに高い研究成果を生み出し、実用化に向けて着実に進めて欲しい。また、DEOS プロセス・アーキテクチャーとの統合が始まっているが、概念実証にとどまらず、実用化のレベルを目指した統合を進めて欲しい。これまでの成果の多くはセキュリティに関する個別要求から発生して DEOS プロセス・アーキテクチャーに統合されているが、今後は DEOS プロセス・アーキテクチャーをよりディペンダブルにするという観点から、D-System Monitor との統合を進め、D-RE のあるべき姿や DEOS プロセスとの連携など、セキュリティを含む広い範囲の研究テーマを開拓し、進めていただけるとなおよい。これを進めての実用化し、普及させることにより、大きな社会的貢献が期待できる。

4－3. 総合的評価

OS の健全性検証、回復機能、セキュア VM、障害予知検知のすべての研究項目について顕著な成果を上げており、高く評価できる。今後、セキュリティ技術を含むより広い範囲でのディペンダビリティー技術への貢献と、DEOS プロセス・アーキテクチャーとのさらなる融合を図ってほしい。