平成 23 年度研究開発成果概要書

「マルウェア対策ユーザサポートシステムの研究開発」

（１）研究開発の目的

本研究開発では、ユーザパソコンに負荷がかかる実行コードの解析を nicter 等の解析機能を有する外部のシステムが担うことにより、効率的なマルウェアの検出および自動駆除の仕組みを実現することを目的とする。

（２）研究期間

平成２１年度から平成２３年度（３年間）

（３）委託先企業

株式会社　日立製作所＜幹事＞、KDDI 株式会社

（４）研究開発予算（百万円）

平成２１年度	２３７（契約金額）
平成２２年度	２２３（　〃　）
平成２３年度	２０９（　〃　）

（５）研究開発課題と担当

課題ア　：検査プログラムに関する研究開発

ア‐１：不正プログラム基本探索アルゴリズムに関する研究開発
（株式会社　日立製作所）

ア‐２：ホワイトリスト化等を用いた高能率探索手法に関する研究開発
（株式会社　日立製作所）

課題イ　：マルウェア駆除ツールの自動生成・最適化・高速検証手法の研究開発

イ‐１：マルウェア駆除ツールの自動生成・最適化手法の研究開発
（株式会社　日立製作所）

イ‐２：マルウェア駆除ツールの安全性の高速検証手法の研究開発
（株式会社　日立製作所）

課題ウ：ユーザサポートプロトコルに関する研究開発

ウ‐１：クライアントサーバプロトコルの設計及び開発

（KDDI 株式会社）

ウ‐２‐１：クライアントエージェントの設計及び開発

（KDDI 株式会社）

ウ‐２‐２：サーバエージェントの設計及び開発　（KDDI 株式会社）

課題エ：課題ア～ウを実環境で有効に機能させるための実証実験

（KDDI 株式会社）

（６）これまでに得られた研究開発成果

(全体)　件　　（当該年度）件

特許出願	国内出願	10	6
	外国出願	6	6
外部発表	研究論文	4	3
	報道発表	1	1
	その他研究発表	17	12
	展示会	6	6
	標準化提案	3	3

具体的な成果

(1) 2011 年 9 月から 12 月まで５校の教育機関と共同でマルウェア対策ユーザサポートシステムのフィールド実験を実施。１０００体の検体を解析し、システムの有用性を確認。「ICSS 研究会」（主催：電子情報通信学会）にて発表。

(2) ネットワークセキュリティに関する代表的な国際会議である RAID (International Symposium on Recent Advances in Intrusion Detection)2011 にて、ユーザサポートシステムの概要について発表し、各国の研究者に対して研究成果をアピール。

(3) マルウェア解析環境の時間経過速度を高速化することで、特定の日時にのみ活動を行うマルウェアの効率的な解析を実現する方式を考案し、特許を出願。