

平成 22 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 nictar 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
平成 22 年度	223

(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	4	2
	外国出願	1	1
外部発表	研究論文	1	1
	報道発表	0	0
	その他研究発表	6	4
	展示会	0	0
	標準化提案	0	0

具体的な成果

- (1) マルウェア対策ユーザサポートシステムの主要機能の開発を完了し、検体の発見から駆除までの一連の基本動作を確認。「マルウェア対策研究人材育成ワークショップ」(主催: 情報処理学会)にて発表。
- (2) サーバ側・ユーザ PC 側のホワイトリストフィルタが連携し、サポートセンタに非マルウェアと判断されたファイルを、ローカルホワイトリストに自動登録する機構を開発し、性能が開発目標(5分以内)を満たすことを確認。「電子情報通信学会総合大会」にて発表。
- (3) ユーザ PC 内から複数の擬陽性ファイルが発見された場合に、ハッシュ値やプロセスの親子関係などに基づきサポートセンタに送信するファイルを絞り込むことで、ネットワーク負荷や演算負荷を低減する方式について、特許を出願。