（事後評価）

暗号通信手順の安全性自動検証に関する研究

（研究期間：平成１２年～１４年）

任期付研究員：大崎　人士（独立行政法人産業技術総合研究所）

○総　評（期待したほどではなかったが一定の成果が得られた研究であった）

本研究は、情報科学における基礎技術を通信工学に応用し、情報システムの安全性を検証する技術について検証するというものである。具体的には、書換系及びツリー・オートマトンの理論による数理的基礎を発展させ、暗号を用いた通信プロトコルで、意図する相手にのみ秘密情報を伝達することができるか（秘密保持性があるか）を自動検証する手法の開発を目指すものである。

本研究において、情報社会における重要課題「暗号鍵の安全受渡し自動検証」について、ツリー・オートマトンの理論的研究に取組み、理論モデル構築という目標設定は評価できる。しかし、自動検証システムの実装はしたものの、具体的な実用システムではなく、理論的成果の効用や実用性などの評価が不十分である。このため、所期の目標が十分達成されたとは言い難く、今後、実用化に向けた更なる研究が期待される。

特に、本研究テーマは理論面より実用面が重要であると考えられ、かかる観点からの計画性が不十分であるという印象も見受けられる。検証自動化のソフトウェア作成に十分な比率で経費配分しているものの、成果報告書にその成果が触れられておらず、研究計画は十分適切であったとは評価できない。今後、成果の活用についても積極的に努力することが望まれる。

一方、本研究における任期制の活用の効果については、短期間で一定の研究成果が得られ、所属研究室における研究の活性化に寄与している面も見受けられることから、概ね効果があったと判断できる。また、所属機関の任期付研究員への支援については、研究立ち上げ時のサポートなど、研究遂行に必要な環境整備は概ね行われたと判断できるが、研究指導という面で不十分な面も見受けられる。

以上により、本研究に係る所期の目標達成に向けては、実用性の観点からの検証が不十分であり、こうした点を踏まえ総合的に判断すると、本研究は期待したほどではなかったが一定の成果が得られた研究であったと評価できる。

＜総合評価：ｃ＞

○評価結果

総合評価	目標達成度	研究成果			研究計画	任期制の活用の効果	所属機関の支援
		科学的・技術的価値	科学的・技術的波及効果	情報発信			
c	c	b	b	a	b	b	b