令和７年度　日本大学危機管理学部　個人研究費　研究実績報告書

所属： 危機管理学部　危機管理学科
資格： 教授
氏名： 鈴木　耕二

研究課題名	虚二次体上に構成される公開鍵暗号系の計算量的安全性評価についての基礎研究
研究目的及び研究概要	RDSAや Guillou-Quisquater署名など、公開鍵暗号系の幾つかは虚二次体上に構成可能であることが知られている。現在のところ、虚二次体上に構成された公開鍵暗号系については十分な研究が実施されておらず、その安全性について不明な点が多い。本研究では、虚二次体上に構成された公開鍵暗号系の計算量的安全性を明らかにする。
研究実績の概要 研究の進捗状況・得られた成果・今後の課題・研究実績等	研究の第一段階として、虚二次体上に構成されたRDSAの解読に要する計算量の上限値を予測した。今後はこの上限値の適正さを計算機実験を用いて検証する。