

「21世紀COEプログラム」(平成14年度採択) 中間評価結果表

機 関 名	中央大学	拠点番号	C17
申請分野	情報・電気・電子		
拠点のプログラム名称 (英訳名)	電子社会の信頼性向上と情報セキュリティ (Research on Security and Reliability in Electronic Society)		
研究分野及びキーワード	〈研究分野: 情報セキュリティ〉(電子社会)(暗号)(コンピュータ・ネットワークセキュリティ)(信頼性)(電子投票)		
専攻等名	理工学研究科 情報工学専攻、電気電子情報通信工学専攻、数学専攻、経営システム工学専攻 理工学研究科電子社会・情報セキュリティ副専攻、中央大学研究開発機構		
事業推進担当者	(拠点リーダー) 辻井 重男 教授 他 26名		

◇拠点形成の目的、必要性・重要性等：大学からの報告書(平成16年1月現在)を抜粋

<本拠点がカバーする学問分野について>

本拠点では、情報セキュリティを、技術、経営・管理、法制度、情報倫理等から成る学際的総合科学として捉える視野の中で、暗号理論、コンピュータ・ネットワークセキュリティ技術、及びそれらの基盤の上に築かれる電子投票システム、地理情報システムなどの電子社会システムの構成法等の技術基盤を中心に研究を推進する。

<本拠点の特色及びその目的等>

- (1) 学際的情報セキュリティ総合科学の体系化について、技術の進歩や社会的環境の変化を考慮しつつダイナミックに検討する。
- (2) 情報セキュリティ総合科学を基礎理論・要素技術層、高信頼コンピュータ・ネットワークシステム層、電子社会システム層に階層化し、本学の多様な人材を結集して研究を推進する。

このような体系的な研究は、電子社会にとって最も緊急性の高い課題の一つである。

<COEを目指すユニーク性>

本拠点は政府のe-Japan重点計画における5本柱の一つである信頼性・安全性を、学術的分野として真正面から取り上げた唯一のCOEである。

総合的視点からの独自性としては、総合大学としての環境を生かした、情報セキュリティ総合科学のダイナミックな体系構築であり、この点では、内外に殆ど例を見ない。

次に、個々のテーマについては、暗号研究者と高い国際的業績を有する数論研究者との協力による超楕円暗号方式の提案や、DNA情報による個人識別など世界の先端を競うユニークな成果を挙げている。アルゴリズムグループでは、浅野教授は権威ある国際論文誌において、最大充足化問題に対し世界最高速の高性能近似アルゴリズムの提案をし、また、山村教授は同じく著名な国際論文誌に引用回数が年間発表された約500編中 第6位の論文を掲載している。

<本拠点のCOEとしての重要性・発展性>

コンピュータのユビキタス化が加速し、それに伴って社会環境が激しく変化していく電子社会において、情報セキュリティの向上は永遠の本質的課題である。例えば、現代暗号は情報秘匿(プライバシー・産業機密の保持)と併せて、認証(人、モノ、文書、金などの情報の真正性保証)という電子社会を推進する役割を担っており、コンピュータやアルゴリズムの進歩を予測した不断の先回り研究が必要である。

<本プログラムの事業終了後に期待される研究・教育の成果>

本拠点は、総合大学としての全学的関心を惹起し、広い学術的・組織的支援体制が確立されている。研究拠点としては、暗号研究と並ぶ主要な分野であるコンピュータセキュリティについて、2003年度より我が国を代表する研究者である土居範久教授を本学情報工学科教授に迎え本プログラムに加えたこと、また更なる人材強化計画も進められていることから、情報セキュリティ技術に関する研究・教育体制が確立されている。

<背景となる当該研究分野の国内外の現状と動向、期待される研究成果と学術的・社会的意義、波及効果等>

情報セキュリティには総合的対策が必要であり、その学問的基盤としての学際的情報セキュリティ総合科学の体系化という発想と総合大学という環境の下での具現化は本拠点独自のものであり、社会的意義は大きい。

個別テーマとしては、超楕円暗号の実用的鍵長の実現は本拠点が先鞭をつけたが、その後、ドイツ、フランスの研究者が追試し、現在切磋琢磨している。これらの成果は将来の社会発展の基盤として期待されている。

また、2004年度に予定している次世代オンライン型電子投票の実証実験は、今後の電子政府・自治体のあり方への示唆を提供できると考えている。

機 関 名	中央大学	拠点番号	C 1 7
拠点のプログラム名称	電子社会の信頼性向上と情報セキュリティ		

◇ 21世紀COEプログラム委員会における評価

(総括評価)

当初目的を達成するには、下記のコメントに留意し、一層の努力が必要と判断される。

(コメント)

来るべきユビキタス社会において極めて重要となる信頼性とセキュリティの問題を暗号理論、システム・ネットワーク、人文・社会学、の多角的視点から総合的に取り組むことを目標にしており、他にみられない特色あるCOEと認められる。学長・拠点リーダーをはじめとして本プログラムメンバーが本COEの社会における重要性を良く認識しており、高い意識を持って教育・研究を推進していることは評価できる。

拠点リーダーのリーダーシップのもとに参加メンバーの研究項目は組織的に構成されているが、暗号理論研究、ネットワーク・システムセキュリティ研究、人文科学・社会科学研究の三大分野間のコミュニケーションをより促進させる必要があると思われるので、一層努力していただきたい。暗号理論研究は極めて高度な数学的知識を有する人材を必要とするので、学内外より優秀な研究者の獲得に不断の努力を行い、研究者層を一層充実させていただきたい。

本COEの理論研究を特徴付ける超楕円関数による暗号理論や量子暗号理論の研究については、必ずしも学界でのコンセンサスが得られている段階には至っていないことに鑑み、今後さらに内外での成果発表を積極的に行い、海外を含めた学界で認知されるよう努めていただきたい。

教育、人材育成についてはセキュリティに関する総合的な実務教育のカリキュラムの構築、教材の作成に取り組んでおり、その教育成果が期待される。今後はそのカリキュラムや教材を当大学の教育のみにとどまらず、広く日本国内、さらに英語化により世界の大学に発信することを期待したい。