２１世紀ＣＯＥプログラム　平成１４年度採択拠点事業結果報告書

１．機関の代表者（学　長）	（大学名）　中　央　大　学	機関番号	３２６４１
	（ふりがな〈ローマ字〉）　NAGAI　KAZUYUKI （氏　名）　永　井　　和　之		

２．大学の将来構想

(1) 大学の将来構想

本学は、「自由で批判精神に満ちた学問研究」を尊ぶ学風の継承と「実学の重視」「開かれた教育」を１世紀余にわたり実践し、多くの優れた人材を輩出してきた。これらの実績を踏まえ、新たに「中央大学21世紀宣言」を採択し、「新しい社会を創造する世界最高水準の大学を目指す」ことを21世紀における本学の目標と定め、具体的には[1]人間性、国際性豊かな人材の育成、[2]世界で活躍するプロフェッショナルの育成、[3]世界レベルでの研究成果の発信・交流、[4]都市・地域と一体となった知的資産の創造と活用、[5]これらの大学づくりを実現するためのキャンパス整備、の５つの目標を定めた。そして特に上記[3]の目標を達成するために以下の中核的戦略を定めた。

＜戦略１　世界的研究教育拠点形成戦略＞

世界的な研究教育拠点の形成戦略は、①社会の要請を的確に捉え、それに応え得る拠点であること、②総合大学の利点と世界規模でのネットワークを生かした拠点であること、③研究成果を教育に十分還元できる場の提供が工夫された拠点であること、の３つを特徴として、それらに合致する幾つかの戦略的研究プロジェクトを2002年から実施することとした。その中でも「電子社会の信頼性向上と情報セキュリティ」は、本学が取り組むべき最重要な課題として学長主導の下で取り組むこととした。

＜戦略２　世界に通用するﾌﾟﾛﾌｪｯｼｮﾅﾙ育成戦略＞

本学は「実学の伝統」の強化を目的に専門職大学院の設置を検討し、2002年に国際会計研究科を創設するとともに、法科大学院については2004年の開設に向けて準備を進めた。

＜戦略３　地域及び産官学連携戦略＞

本学の主な拠点のひとつである多摩地域に、新たな魅力を創出することを目的として「学術・文化・産業ネットワーク多摩」を2002年に設立し、47大学、33団体の参加を得て具体的な地域連携活動を開始した。また、産官学共同の活発化は、学部、大学院、研究所等において推進しており、なかでもその専門実施機関として1999年に設置した研究開発機構では、学内外の多彩な研究員の参加のもと、大型学際的共同研究プロジェクトが活動を行ってきた。研究開発機構におけるこの成果は、本学の研究教育活動全体の活性化にも寄与しており、それらをさらに発展させることを計画した。

(2) 学長を中心としたマネジメント体制

学長は、学部長会議及び大学院研究科委員長会議の主宰者として、研究教育に係る諸課題を全学的視点に立った政策としてまとめる主導的な役割を果たしている。さらにその機能の高度化を図るため、学部長補佐制度、学長専門員制度を新設し、学部長会議、研究科委員長会議とともに学長専門員が学長を中心としたマネジメント体制の中核的組織を形成する体制を整えた。さらに総合的な将来構想とその具体的実施計画を策定する総合企画委員会(学長が委員長)と教学各機関の代表者及び学部選出委員で構成される研究・教育問題審議会が、学長の政策形成を支える体制をとった。

＜拠点形成の支援＞

①学内予算措置：学長主導の下に、2002年度予算において、「21世紀COE基盤整備費」として5,000万円の予算措置を講じた。

②研究教育組織の改編：独立研究科としての電子社会システム研究科の設置を構想した。さらに、情報セキュリティ、ナノテクノロジー、環境理工学、防災・危機管理工学、データ科学の５つの副専攻を2003年に開設することを計画した。これら一連の大学院改革は、学際領域の新分野と８専攻で構成している理工学研究科における専攻横断的な新分野の開拓を目指すものとして、本学が世界的な研究教育拠点を形成する上での戦略的布石とした。

③施設・スペースの整備：全学的キャンパス整備計画の一環として、理工学部、大学院理工学研究科、理工学研究所、研究開発機構等による研究教育活動を一層充実させ、世界レベルの研究成果の発信・交流を行う拠点にふさわしい施設充実を図るため、後楽園キャンパスに新棟を建設し、本学が進めている戦略的研究プロジェクトに必要な施設の多くを新棟に設置することを計画した。

④研究者及び研究支援者の措置：国外研究者の招聘については、外国人客員教員制度、国際共同研究制度などの諸制度を活用し、研究支援体制については、大学院学生をリサーチ・アシスタント(RA)、ティーチング・

アシスタント(TA)として採用することとした。

⑤国内外有識者アドバイザリーグループの設置：世界的な研究教育拠点の形成にあたっては、社会的受容性の高い研究成果を創出するために、人文・社会科学系研究者やその他の有識者の客観的評価や助言を得ることを目的として、アドバイザリーグループを設置することとした。

３．達成状況及び今後の展望

(1) 大学の将来構想

「新しい世界秩序の創成」、「循環型社会の構築」などの人類の持続可能な発展を巡る諸課題は、従来の科学技術水準や学術体系だけでは充分な対応・解決が困難になってきており、新たな学際パラダイムへの転換が求められている。こうした中で本学は、前記「宣言」を基に「世界の中で存在感のある大学」として、①個性あふれる知的空間を創造すること、②人間性豊かで国際的に通用する人材を輩出すること、③実地応用の学問(社会のための科学)の伝統をふまえ地域・社会に貢献することをミッションとし、学長を中心として次の3点に注力した大学改革に着手している。本学はこれを目標達成に向けた第二弾の戦略として位置づけている。

＜世界的教育研究拠点の形成とﾌﾟﾛﾌｪｯｼｮﾅﾙの育成＞：本項目は前記２．に掲げた戦略１、戦略２にあたる。研究においては、基礎研究の充実を図る一方で、「安全・快適な暮らしの実現」をキーワードに21世紀COEプログラム拠点である情報セキュリティのほか、環境、危機管理、国際関係を重点4分野として定め、新たな学際的総合科学の構築を目指している。なお、前記の３つの戦略的研究プロジェクトについては、研究拠点となるセンターを理工学研究所に設置し、学部及び研究科との連携のもと研究教育活動を展開している。そしてその成果としては、論文の発表はもとより、21世紀COEプログラム、科学技術振興調整費、特許化支援制度などの競争的資金に採択されるなど、着々と成果をあげている。また、専門職大学院等では、実学とキャリアの融合を志向し、これまでに国際会計研究科、法務研究科、公共政策研究科を開設してきた。さらに、2008年度に向けて戦略経営研究科の開設を進めている。

＜最高水準の教育研究をサポートする環境・経営基盤の整備＞：専門職大学院の更なる展開や、大学院と既存学部や研究機関との連携を強化する必要性に鑑み、都心キャンパスを中心に、国際的なコンソーシアムの展開や若手研究者の育成に資する施設・設備の充実を図る。また、より高度な教育研究を推進するために有力な研究者を増強するとともに、意欲の高い学生を確保するためにアドミッションポリシーの浸透と入試改革にも注力し、経営基盤の改善・強化を図る。

＜地域ネットワークの展開と社会への還元＞：本学は地域貢献を重視しており、「学術･文化･産業ネットワーク多摩」の設立、2006年には文京区と教育の包括提携を行うなど、生涯学習講座や産学連携を通じた地域社会の活性化に寄与している。また、研究成果の還元においては、特許の出願件数などが伸びてきている。今後は、リポジトリ機能を含む研究者・研究シーズ発信システムを整備し、積極的な情報発信にも注力していく。

(2) 学長を中心としたマネジメント体制

本学は、総長・理事長・学長を中心としたマネジメント体制を執っている。現在は、学長が総長を兼務しており、本拠点形成に係る学内予算措置、施設・スペースの整備等の法人事項は、総長・理事長が密接に連携し、柔軟かつ迅速な意思決定を行っている。他方、教育研究組織の改編や研究者・教員・教育研究支援者の任用等の教学事項は、教学の長である学長が強力なリーダーシップを発揮し全教学組織を取り纏めた。

＜拠点形成の支援＞

①学内予算措置：学長主導の下に毎年度「21世紀COE基盤整備費」として予算措置を講じた。今後も必要な予算措置を講じ、本拠点活動を積極的に支援する。

②研究教育組織の改編：2003年に理工学研究科に電子社会･情報セキュリティ副専攻を開設したのに加えて、2007年に情報セキュリティ科学専攻(独立専攻)を開設した。また、研究部門の強化のために2006年に「情報セキュリティ研究センター」を理工学研究所に設置した。

③施設・スペースの整備：2003年、後楽園キャンパスに竣工した新３号館を世界的レベルの研究成果の発信、交流拠点として位置づけている。本拠点形成においても新３号館を中心として、その中核を担う情報工学専攻などを集中させ、施設面からも拠点形成を支援した。

④研究者及び研究支援者の措置：本拠点形成を視野に入れた専任教員人事により、有力な研究者の採用を実現したほか、客員教員制度、国際共同研究制度等の諸制度の積極的な活用や、研究拠点形成費により有力な研究支援者を採用するなど、研究基盤の強化を図った。今後も諸制度を利用して有力な研究者を招聘する。

⑤国内外有識者アドバイザリーグループの設置：有識者の客観的評価や助言を得ることを目的としたアドバイザリーグループと知的財産の管理・活用のための産学官連携・知的財産戦略本部を設置した。

様式２
【公表用】

２１世紀ＣＯＥプログラム　平成１４年度採択拠点事業結果報告書

機 関 名	中央大学	学長名	永井和之	拠点番号	Ｃ１７
１．申請分野	Ａ〈生命科学〉　Ｂ〈化学・材料科学〉　Ⓒ〈情報・電気・電子〉　Ｄ〈人文科学〉　Ｅ〈学際・複合・新領域〉				
２．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〉(暗号)(信頼性)(電子認証)(ｾｷｭｱﾈｯﾄﾜｰｸ)(電子投票)				
３．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、中央大学研究開発機構				

４．事業推進担当者　　計　29名

ふりがな 〈ローマ字〉 氏　名	所属部局(専攻等)・職名	現在の専門/学　位	役割分担(事業実施期間中の拠点形成計画における分担事項)
(拠点リーダー)			
TSUJII SHIGEO 辻井　重男	本学理工学部・教授(大学院理工学研究科情報工学専攻)から本学研究開発機構・機構教授に変更（平成16年4月1日）	暗号・情報ｾｷｭﾘﾃｨ/工学博士	総括、電子社会論、暗号理論
ASANO TAKAO 浅野　孝夫	本学理工学部・教授(大学院理工学研究科情報工学専攻)	ｱﾙｺﾞﾘｽﾞﾑ/工学博士	ネットワークの信頼性向上のためのアルゴリズム
MAKINO MITSUNORI 牧野　光則	本学理工学部・助教授から教授(大学院理工学研究科情報工学専攻）に昇格（平成16年4月1日）	ｺﾝﾋﾟｭｰﾀｸﾞﾗﾌｨｯｸｽ/博士（工学）	情報セキュリティシステムの可視化
DOI NORIHISA 土居　範久	本学理工学部・教授(大学院理工学研究科情報工学専攻) 追加（平成15年10月1日）	ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨ/工学博士	情報ネットワークの高信頼化とセキュリティポリシー
SHINODA SHOJI 篠田　庄司	本学理工学部・教授(大学院理工学研究科電気電子情報通信工学専攻)	情報ネットワーク/工学博士	移動通信ネットワークの信頼性向上
CHAO JINHUI 趙　晋輝	本学理工学部・教授(大学院理工学研究科電気電子情報通信工学専攻から大学院理工学研究科情報工学専攻へ所属変更；平成16年4月1日）	暗号理論/工学博士	楕円・超楕円暗号理論
YAMAMURA KIYOTAKA 山村　清隆	本学理工学部・教授(大学院理工学研究科電気電子情報通信工学専攻)	ｱﾙｺﾞﾘｽﾞﾑ/工学博士	システムの高信頼化アルゴリズム
SUGIYAMA TAKAKAZU 杉山　高一	本学理工学部・教授(大学院理工学研究科数学専攻)	統計学/理学博士	電子データの信頼性検証
KONNO HIROSHI 今野　浩	本学理工学部・教授(大学院理工学研究科経営システム工学専攻)	金融工学/工学博士	電子金融システムの高信頼化
SAITO TADAO 齊藤　忠夫	本学研究開発機構・機構教授	情報通信/工学博士	情報ネットワークの高信頼化
HUZII MITUAKI 藤井　光昭	本学研究開発機構・機構教授より本学大学院理工学研究科・客員教授に変更（平成17年4月1日）	時系列解析/理学博士	暗号理論における乱数検定
TAGUCHI AZUMA 田口　東	本学理工学部・教授(大学院理工学研究科情報工学専攻）追加（平成15年4月1日）	情報数理/工学博士	地理情報システム
IMAI KEIKO 今井　桂子	本学理工学部・教授(大学院理工学研究科情報工学専攻)	ｱﾙｺﾞﾘｽﾞﾑ/理学博士	地理情報システムのセキュリティ
SHIRAI HIROSHI 白井　宏	本学理工学部・教授(大学院理工学研究科電気電子情報通信工学専攻)	通信工学/Ph. D.	電磁波漏洩の解析とその可視化
SEKIGUCHI TSUTOMU 関口　力	本学理工学部・教授(大学院理工学研究科数学専攻)	代数幾何/理学博士	代数幾何の暗号理論への応用
SUWA NORIYUKI 諏訪　紀幸	本学理工学部・教授(大学院理工学研究科数学専攻)	代数幾何/理学博士	平成15年3月20日付交付申請にて「整数論の暗号理論への応用」から「数論的代数幾何の暗号理論への応用」へ変更
MOMOSE FUMIYUKI 百瀬　文之	本学理工学部・教授(大学院理工学研究科数学専攻)	整数論/理学博士	整数論の暗号理論への応用
KUME HITOSHI 久米　均	本学理工学部・教授(大学院理工学研究科経営システム工学専攻)	品質工学/工学博士	電子社会システムに対する安全学の構築
KAMAKURA TOSHINARI 鎌倉　稔成	本学理工学部・教授(大学院理工学研究科経営システム工学専攻)	統計学/工学博士	暗号理論における乱数検定
NAKAJO TAKESHI 中條　武志	本学理工学部・教授(大学院理工学研究科経営システム工学専攻)	品質管理/工学博士	電子社会システムにおける過失の軽減
OKAMOTO TATSUAKI 岡本　龍明	本学大学院理工学研究科数学専攻・兼任講師（NTT研究所）	暗号理論/工学博士	公開鍵暗号の安全性証明
ITAKURA YUKIO 板倉　征男	本学研究開発機構・客員研究員	情報セキュリティ/博士（工学）	DNA情報による個人識別
MATSUO KAZUTO 松尾　和人	本学研究開発機構・機構助教授より教授に昇格（平成16年4月1日）	暗号理論/博士（工学）	楕円・超楕円暗号理論
DOI HIROSHI 土井　洋	本学研究開発機構・機構助教授	暗号理論/博士（理学）	電子投票・電子證券システム
UCHIDA KATSUYA 内田　勝也	本学研究開発機構・機構助教授	情報セキュリティ/ 18年7月26日博士（工学）取得	セキュリティポリシー
HIROTA OSAMU 広田　修	本学研究開発機構・客員研究員（玉川大学教授）	量子情報科学/工学博士	量子暗号・量子計算
HORIBE MASAO 堀部　政男	本学大学院法務研究科・教授追加（平成17年4月1日）	情報法/法学博士	電子社会論
HOSONO SUKEHIRO 細野　助博	本学総合政策学部・教授(大学院総合政策研究科総合政策専攻)	電子自治体/経済学修士	ネットワーク多摩による実証実験
IRI MASAO 伊理　正夫	本学理工学部・教授(大学院理工学研究科情報工学専攻)退職（平成15年3月31日）	情報数理/工学博士	地理情報システム

５．交付経費（単位：千円）千円未満は切り捨てる　（　　）：間接経費

年　　度(平成)	１４	１５	１６	１７	１８	合　　計
交付金額(千円)	112,000	103,000	103,000	96,000（9,600）	88,070（ 8,807）	502,070

６．拠点形成の目的

電子社会では、多様な組織の間の壁が低くなって人々の活動の自由度が増大する。これは技術の面から見て必然ともいえるが、電子社会の普遍的理念として自由の拡大を挙げることも出来よう。しかし、自由の拡大は他方で様々な不安定性や不安要因を孕むことも不可避であり、安全で活力に満ちた電子社会の構築に向けて、理工学と人文・社会科学の全ての面からの総合的な研究を推進していかねばならない。

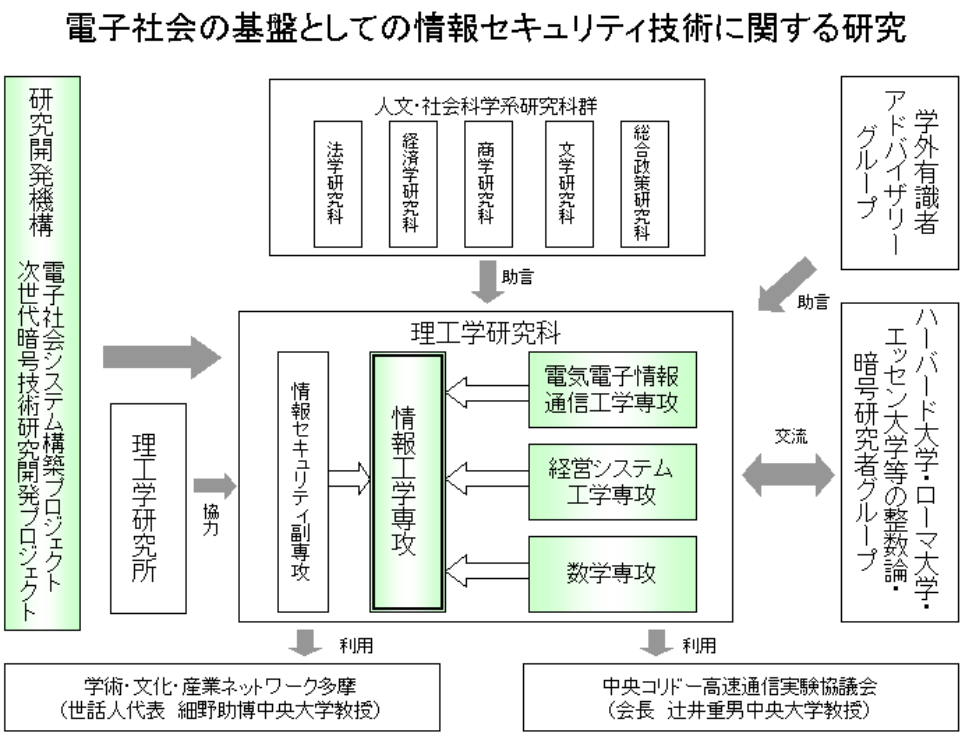
本拠点リーダー辻井重男教授は、日本学術振興会の未来開拓研究推進事業における唯一の例外ともいえる人文・社会科学系プロジェクト群を束ねる「電子社会システム推進委員会」（1998年発足）の委員長を務める中でこのことを痛感し、中央大学研究開発機構の中に堀部政男法学部教授や細野助博総合政策学部教授など社会科学系研究者も含む「電子社会システム構築プロジェクト」を設置して、学際的総合的研究を推進してきた。

研究開発機構はTLOではなく、外部資金のみにより学・官・産が共同研究を進めている中央大学独自のユニークな組織であり、現在年間約3.5億円の資金で10プロジェクトが進行している。

さて、今後電子社会がどのような形で発展していくにせよ、人々が自由に活動するための舞台は強固で安心できるものでなければならない。少なくとも電子社会の技術的基盤は高い信頼性と安全性を備えていることが強く要請される。

中央大学としては、上記の電子社会に対する総合的研究を進める一方で、とりわけ信頼性と情報セキュリティの重要性を認識して、情報工学専攻と電気電子情報通信工学専攻、数学専攻の研究者等が研究開発機構において外部資金を導入して暗号理論を中心とするプロジェクトを立ち上げ、安全性の高い楕円・超楕円暗号の設計法などの分野で多くの研究成果を挙げ、国際会議等で発表してきた。この分野では、フランスのエコールポリテクニーク、ドイツのエッセン大学と並ぶ研究拠点を形成している。また中央大学理工学研究所においては「暗号理論とそれを支える代数曲線」研究会を発足させ、工学者と数学者による学際的研究を進めている。そして、本研究会と研究開発機構のプロジェクトが協力して楕円暗号やそれに関係の深い整数論や代数幾何の分野で世界的に著名な研究者を招き、研究交流を重ねてきた。2001年8月には志村-谷山予想（楕円曲線はモジュラーであろう）を最終的に解決したBrian等3名を、また2002年2月にはFreyの楕円曲線（志村-谷山予想、その副産物としてフェルマーの最終予想の解決のきっかけとなった代数曲線）を提案したFreyや、楕円暗号の安全性検証に必要なSchoofのアルゴリズムで知られるSchoofなど4名の研究者を招いてシンポジウムを開催し、内外から多くの暗号研究者と数学者が出席して議論を深めた。これは、申請前の研究活動の一端であるが、本計画ではこうした研究を深めると共に、より広い視野の下に数学専攻や経営システム工学専攻に豊富な人材を擁する統計学や安全学等の分野、及び信頼性の高いネットワーク構成論等を含め、具体的な電子社会システムへの利用を図りつつ電子社会の安全な基盤形成に向けて体系的研究を推進することを目的とした。

本計画推進のための体制を下図に示す。



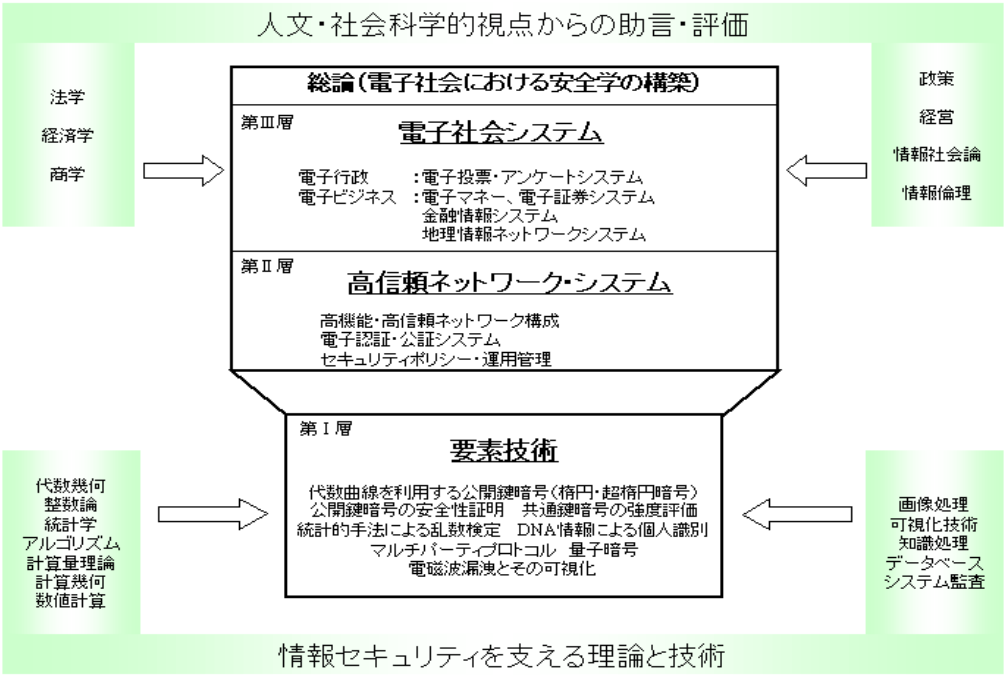
７．研究実施計画

電子社会の安全を脅かす脅威には災害、故障、過失、故意（悪意）が考えられるが、本計画では故意を中心に災害、故障、過失も可能な限り考慮して電子社会の信頼性と情報セキュリティを向上させるための技術的対策を総合的に研究する予定であった。

本研究の対象はおおよそ下図の太線内のように総論（電子社会における安全学の構築）、及び３階層で示される。３階層は縦方向にも互いに強く関連している。そのことを、暗号を例に説明する。

電子社会における暗号技術は秘匿と認証という２つの役割を担っている。秘匿はプライバシや産業機密を守るために行われ、認証は、サイバースペースという不可視の世界において本人確認や文書の原本性確認をはじめ、電子マネー、知的財産物あるいは全てのモノに関する情報の真正性を保証することを意味しており、ユビキタス社会においては価値あるものの全てに要求される機能である。

認証は主に楕円・超楕円暗号などの公開鍵暗号によって第Ⅱ層の電子認証（公開鍵基盤）として実現される場合が多く、第Ⅲ層における全ての電子社会システムの基盤となっている。上に掲げた研究対象の多くは、既に本学の情報工学等の諸専攻や研究開発機構において研究を重ねてきたテーマであるが、拠点形成にあたってはこれらの成果を発展させつつ、上記の階層構造の下に有機的に連携させて統合化し、電子社会の強固な基盤を構築するという使命感を持って研究を推進する予定であった。また、本学の社会科学系の優れた研究者達の助言を得つつ研究を進め、研究期間の後半においては本学が中核となって運営している「学術・文化・産業ネットワーク多摩」及び拠点リーダーが会長を務める「中央コリドー高速通信実験協議会」のネットワークを活用して、例えば次世代電子投票・アンケートシステムの技術的・社会的実験も行いたいと考えていた。



研究の階層	研究課題	H14	H15	H16	H17	H18
総論	電子社会における安全学の構築	事業担当者全員により、下記の3階層の成果と相互連携しつつ討議				
第Ⅲ層 電子社会システム	電子行政	電子投票システム			電子投票・アンケートシステム	
	電子ビジネス・金融システム	電子金融システム				
	地理情報システム				ネットワーク多摩による利用実験	中央コリドー高速通信実験協議会
第Ⅱ層 高信頼ネットワーク・システム	セキュリティポリシー	リスク分析	脆弱性データベースの研究			
	システム監査・ヒューマンエラー				トータルセキュリティ向上に対する提言	
	電子認証・公証システム	DNA情報と電子認証・公証				
	高機能・高信頼ネットワーク構成	移動体無線ネットワークの高信頼設計法				
第Ⅰ層 要素技術	マルチパーティプロトコル	秘密分散・ZKIP				
	楕円・超楕円暗号の設計法	代数曲線の研究と暗号設計への応用				
	暗号の証明可能安全性					
	乱数の統計的検定，量子暗号・量子計算	暗号の乱数性と強度，ハッシュ関数 量子暗号・量子計算				
	DNA情報による個人認証	DNA情報に対する統計的検定・DNA情報の管理と倫理規定				
	電磁波漏洩とその可視化					

８．教育実施計画

中央大学における情報セキュリティ分野の人材育成は下図に示す組織的連携の下に進める計画であった。本計画の特長的な点は、

(1) 産業界との交流：社会人博士後期課程学生（企業等に在籍のまま入学）の積極的受け入れ
(2) COE を中核とし理工学研究科及び研究開発機構との共同あるいは一体的研究を通じての人材育成
(3) 理工学研究科における情報セキュリティ副専攻（博士前期・後期課程）の設置による人材育成
(4) 工学と数学、工学と人文・社会科学との学際的研究を通じて深い専門性と広い視野を持つ人材の育成

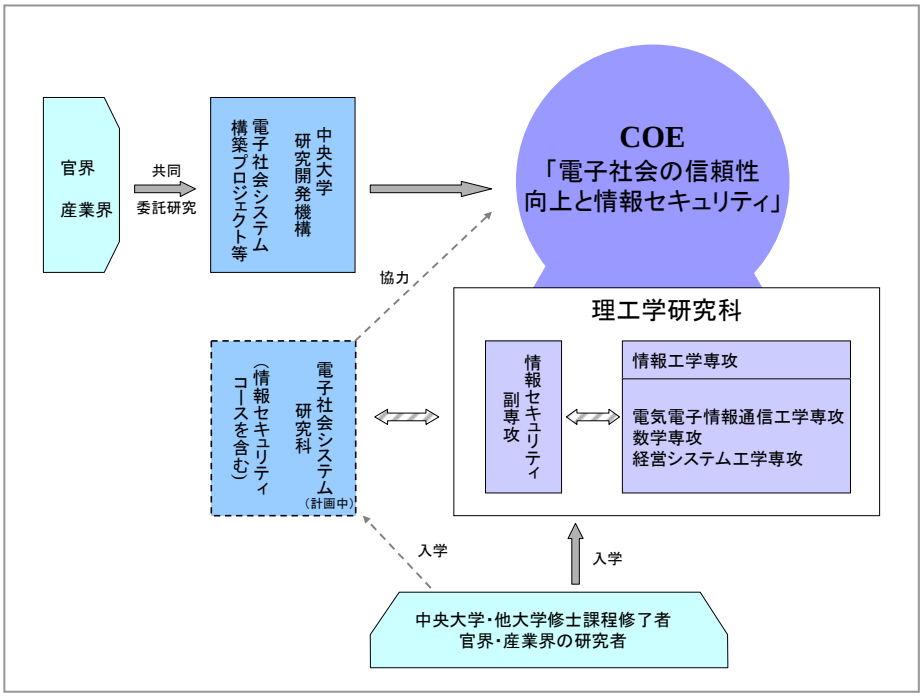
が挙げられる。(1)～(4)について以下順次説明する。

(1) 本拠点計画に参加する情報工学、電気電子情報通信工学、数学、経営システム工学の4専攻が1999年度から 2001 年度の3年間に理学・工学の博士の学位を授与したものは、社会人で博士後期課程学生であった者 10 名を含め合計 19 名であり、卒業後、大学あるいは産業界において活躍中である。また、在学中の者は社会人14名を含め合計45名である。今後も、理工学研究科が中央大学後楽園キャンパスにあるという地の利を活かし、産業界から社会人博士後期課程学生を積極的に受け入れ、情報セキュリティ分野の人材育成に貢献したい。

(2) 中央大学研究開発機構では通信・放送機構等から受け入れた資金により、情報セキュリティ分野で3つのプロジェクト研究を進めてきたが、これらのプロジェクト研究に申請時社会人博士後期課程修了者5名・在学者2名が客員研究員として（学位取得者のうち1名は研究開発機構助教授として）、また通常の博士後期課程学生2名が研究補助員（給与が支払われる）として参加しており、理工学研究科と研究開発機構は密接に連携して研究を推進していた。本拠点の採択によって、COEを中核とし、これらの機関を連携させつつ、より高度で総合的な研究を展開し得ると考えている。

(3) 暗号の研究については、我が国は世界の先頭集団を走っていたが、暗号技術は別として情報セキュリティ全般については、国民の意識が最近まで低かったこともあって、我が国の情報セキュリティ教育は米国等に比べて遅れ気味であり、大学院で情報セキュリティ専攻をもつ大学は存在していなかった。中央大学大学院理工学研究科では、このような状況を憂慮し、情報セキュリティ分野の人材育成を目的として、電子社会・情報セキュリティ副専攻を 2003 年度より発足させた。電子社会・情報セキュリティ副専攻は技術のみでなく、システム監査や法制度も含めた学際的副専攻であり、大学院生とともに社会人受け入れを念頭において、研究者及び高度な専門職業人の育成を目指した。本副専攻は、現在講義のみならず学生の研究指導も客員教授によって行っている。本拠点は、既存の諸専攻に加えて、本副専攻とも連携しつつ、研究を通じて人材育成を推進することが可能となり、電子社会の発展に貢献できる。

(4) 理工学研究科数学専攻には代数幾何、整数論分野で著名な、そして暗号理論の構築に積極的関心を示す 3 名の数学者がおり、暗号研究を支えてきた。本拠点ではこれに統計学の研究者も加えた学際的研究を進め、また、電子社会システム層については人文・社会科学系の研究者から適切な助言を得て、深い専門性と視野の広さを持つ人材を育成したい。



９．研究教育拠点形成活動実績

①目的の達成状況

1)世界最高水準の研究教育拠点形成計画全体の目的達成度

本拠点が2002年度に採択されて以来、本学は全学を挙げて、研究と若手研究者の育成に取り組んできた。その結果、暗号と情報セキュリティの基礎理論からネットワークセキュリティなど応用分野まで、著しい研究成果が得られたと同時に、情報セキュリティ総合科学という新しい学問の体系化と構築を目覚しく進展させ、若手研究者を多数育成した。これらにより、想定以上の成果を上げることができた。

2)人材育成面での成果と拠点形成への寄与

現在、官・民・学の様々なレベルにおいて、電子政府に対応できる人材、情報セキュリティに明るい企業経営者、法的知識や経営的視野を有する情報セキュリティ人材が不足しており、こうした人材の育成が多く求められている。本拠点は、我が国の政府が提唱する「e-Japan」戦略の重点計画の一つである「情報セキュリティ人材の育成」に対して、積極的に活動を行ってきた。

・COE研究員、PD、RAの積極的雇用

情報セキュリティ人材の育成について、本拠点では、若手の研究者の育成をめざして事業推進担当者の所属する大学院理工学研究科の各専攻に所属する将来の研究者となるべき博士後期課程の学生を対象にResearch Assistant(RA)を募集し、研究助成と研究成果の発表のための学会出張旅費や論文投稿助成を行った。この5年間にのべ51名のRAを採用し、このうち現在までに15名が博士の学位を取得している。これらのRAの５名は、優れた研究業績を収め、学会賞を受賞している。また広く学内外の博士後期課程の修了者を対象に、将来の情報セキュリティ関連の主たる研究者となりうる人材を育成すべく、COE研究員やPost Doctoral Fellow (PD)を募集し、この５年間にのべ31名を雇用し、国内外の国際会議、シンポジウムや各種研究会への研究発表や論文投稿を積極的に行った。こうした助成金額は、5年間で総額約２億３千万円であり、全交付額の約５割の交付金を若手の研究支援に使用した。

・情報セキュリティ・情報保証 人材育成拠点との連携

本拠点は、2003年度から５年間の予定で開始された文部科学省科学技術振興調整費 中央大学研究開発機構「情報セキュリティ・情報保証 人材育成拠点」と密接に連携しつつ、実践講座や特別研究コースを開設してきた。各種の講座では、暗号と電子認証、ネットワークセキュリティから電子社会の法と経済、セキュリティマネージメントと著作権保護まで幅広く提供している。例えば2003年12月19日から開催されたシンポジウム「情報セキュリティにおける研究・人材育成拠点形成へ向けて」で併催された特別研修コース「電子社会システムと情報セキュリティ」においては、３日間で22時間の講義からなるコースを開設し、７割以上の受講とレポート提出による判定を行った結果、146名をコース修了と認定した。また合計36回の実践講座を開設し、のべ762名の修了生を輩出した。

・電子社会・情報セキュリティ副専攻の新設

情報セキュリティ人材の不足と実務者養成の必要性から、本拠点に集約した事業推進担当者を中心にして、2003年度から大学院理工学研究科の中に博士課程前期課程の学生を対象に、電子社会・情報セキュリティ副専攻を新設した。この副専攻制度は、既存の理工学研究科の主専攻の教育研究を行うとともに、情報セキュリティという新しい分野の学際的な特徴を生かした横断的なプログラムを、主専攻の教育カリキュラムを補完するように開設し、副専攻が定めた必要単位を修得し、作成したリサーチペーパの審査に合格すると、副専攻の修了証が取得できる制度である。本副専攻は、情報セキュリティ分野の学際的カリキュラムを編成し、電子ビジネスや電子政府・自治体あるいは電子医療等の分野で活躍できる人材の育成を図ってきている。翌年の2004年度からは博士課程後期課程の学生もこの副専攻を履修できるようにしており、2006年度までに36名の修了生を輩出した。

・先導的ITスペシャリスト育成推進プログラムへの参加

学生参加型の産学NPO連携研究プロジェクト科目を中心に、連携企業やNPOでのインターンシップ科目を通じてソフトウェア構築の実践的スキルを獲得することを目的とした研究教育プログラムとして、慶応義塾大学などと連携して、標記の育成推進プログラムを2006年度から開始した。このプログラムでは、遠隔と対面教育融合型の共通プロジェクトレビューを毎学期行うことにより、幅広い視点で先端的な情報システムを理解でき、組織において先導的な役割を担う人材に必要な表現能力、交渉能力、マネジメント能力を磨く。最先端のアプリケーションの開発を研究プロジェクトのテーマとして取り上げ、最新の研究成果を生かしたソフトウェア開発を実践していく。

・情報セキュリティ科学専攻の新設

中央大学として、本拠点の成果を引き続き生かしていくために、事業推進担当者6名が本学大学院理工学研究科内で異動し、2007年度に「情報セキュリティ科学専攻」博士後期課程を新設した。初年度から定員を超えた入学者を迎えるなど順調な滑り出しとなり、今後も情報セキュリティ科学分野の研究教育を継続する。

・セキュリティ情報の可視化装置の導入

本拠点では、３面没入型バーチャルリアリティ(VR)設備CAVE (以下、ChuoCAVE)を導入した。ChuoCAVEは３台のコンピュータが生成するCG映像を時分割立体視方式で提示し、液晶シャッタ眼鏡を利用して体感する装置である。ChuoCAVE操作者の眼鏡ならびにコントローラには磁気センサが付けられ、位置ならびに方向の６自由度をそれぞれリアルタイムで計測している。この計測結果を踏まえて生成する映像を逐次変更しているので、仮想環境中で操作者の意思を反映した動きを実現している。

ChuoCAVEは「セキュリティ情報の可視化」の研究のために導入された。電子社会が発展している現在、提示される情報はますます複雑化し、通常の２次元ディスプレイでは同時に表示が困難な事例が増えてきている。また、平面薄型ディスプレイに続く次世代の映像表示装置の候補の一つとして「立体視ディスプレイ」が挙げられていることもあり、情報を効率よくかつ理解しやすく立体視するための技術を構築することが、本拠点にとっても重要と判断した。

これまでに得た、ChuoCAVEならびに関連設備を用いた情報の可視化・立体視化の主な研究成果としては、既に

(1)無線LANに代表される、高周波数電磁波伝搬を利用する無線通信システムの到達性(信頼性)ならびに危険性(漏えいの可能性)の概況可視化(ジャーナル掲載１件、国際会議発表論文7件、報道１件、他)
(2)入力インタフェース改良による操作性の向上(国際会議発表論文１件、他)
(3)立体視情報の効率的伝送と可視化(国際会議発表論文１件)
(4)操作者の視点・視野を考慮した大量形状情報の効率

的立体視化(国際会議発表論文１件、他)
がある。本拠点の成果を多数の本拠点訪問者がChuoCAVEで観覧した。すなわち、本拠点の研究成果の効果的な発表手段としても位置付けられる。

また、(1)で得られた知見をもとにして、安全・安心な電子社会構築の一助となるセキュリティカメラや人間による視認性の数値化方法についても成果を得た(国際特許出願１件、国内特許公開１件、国際会議発表論文１件)。

研究だけではなくChuoCAVEは教育にも利用されており、本拠点の母体の一つである情報工学専攻博士前期課程「コンピュータグラフィックスとバーチャルリアリティ」ならびに「システム解析と可視化」にはChuoCAVE上でのコンテンツ制作が履修生に課せられている。また、理工学部情報工学科１年生全員に、必修科目「情報工学基礎演習」にてChuoCAVE利用テーマが与えられている。さらに、ChuoCAVEを核として立体視環境の整備を継続しており、これらを用いたプロジェクト型演習科目も情報工学科・情報工学専攻を中心にして計画中である。

以上の通り、ChuoCAVEは導入の目的である「セキュリティ情報の可視化」で多くの成果を得、加えて関連分野の研究教育に多大なる貢献を果たしており、今後も有効活用が期待される。

3)研究活動面での新たな分野の創成と、学術的知見等

研究活動の一例としては、高度な数学的概念を必要とする超楕円公開鍵暗号に関して、趙、松尾、辻井を初めとする暗号理論研究者と、百瀬、関口等の数学専攻の整数論・代数幾何学の研究者等の事業担当推進者等が協力して世界をリードする成果を挙げ、次世代暗号としての超楕円暗号の基礎理論と実装技術を確立させた。また、多次多変数暗号やDNAによる個人認証では、目覚しい進展を遂げている。

また、IT社会において、従来の科学技術水準や学術体系だけでは充分な対応・解決が困難になってきた、様々な価値と利害の対立状況を克服するという問題意識の下に、新たな学際パラダイムへの転換が求められている中で、情報セキュリティの総合科学としての体系化について考察を深め、「情報セキュリティ総合科学」という新しい学術分野を創成し、その概念形成、課題抽出と体系化に成功した。

4)事業推進担当者相互の有機的連携

情報セキュリティにおける、伝統的な分野では対処できない新しい課題の解決は学際的な協力を得て初めて可能である。本拠点では、まず、超楕円暗号グループにおいては、世界的整数論の権威である伊原康隆先生を始めとする数学者と工学者との理工融合型研究体制の下で研究成果を挙げてきた。さらに、多次多変数暗号方式やプロトコルなど暗号基礎理論から、網膜、虹彩、指紋などの個人識別技術、セキュアOS、セキュアプログラミング、IPv6や次世代通信のセキュリティ、電磁波漏洩、脆弱性データベースなどの応用技術との協力連携によって、多岐にわたる研究成果が生まれた。

他方、個人情報に対する利用と保護の相克などに見られるように、IT社会は、自由（効率性・利便性）、安全、プライバシという互いに相克する要求課題の解決を迫られている。これらの相互に矛盾する課題を高度にバランスさせつつ解決するために、本拠点では、多様な要素技術をベースに法制度、経営管理とモラル・心理など人間系を強く結合させて相乗効果を生み出すための情報セキュリティ総合科学を構築した。

5)国際競争力ある大学づくりへの貢献度

本拠点は、毎年積極的に国際会議、シンポジウムやワークショップを開催してきた。また研究交流のために本拠点を短期訪問し、学術講演会を行う外国人研究者も69名に上った。これらの活動は、本学の研究成果を広く世界の研究者に知らせるだけでなく、海外における本学の認知度も格段に上昇し、大学の国際競争力の向上に貢献した。また、著名な学者のみならず、現在活躍中の若手の研究者による学術講演や本学の若手研究者との学術交流、相互派遣は、若手研究者によい刺激と経験を与え、国際的に活躍する原動力となっている。

6)国内外に向けた情報発信

本拠点の成果ならびに活動の国内外に向けた情報発信としては、第一に研究成果の査読付論文誌、国際会議、国内会議等による公表を積極的に進めたことが挙げられる。個別成果だけではなく、例えば、電子情報通信学会論文誌 Vol.J87-A, No.6「マルチメディア社会における情報セキュリティ論文特集」において、『電子社会を推進する情報セキュリティ総合科学のパラダイム』が招待論文として掲載されるなど、拠点全体に関わる成果も積極的に公表した。また、事業推進担当者が国内外の会議に講演者として招待されることも多数あり、これらを通じて電子社会の信頼性向上と情報セキュリティに関する各研究領域の成果を発信した。さらに、本拠点は会議の共催ならびに企画提案を積極的に進めた。例えば、2005年９月に情報処理学会・電子情報通信学会が共催した第４回情報科学技術フォーラムにて、シンポジウム「国家的課題としての情報セキュリティ人材育成」を企画実施した。また2006年６月に開催した第25回日本シミュレーション学会大会を日本シミュレーション学会と共催した。

これらに加えて本拠点全体の活動について国内外に周知する活動として、本拠点主催による国際・国内シンポジウムを実施した。国際シンポジウムでは海外研究者を招いて本拠点の活動に触れる機会を作り、国内シンポジウムは研究者だけではなく一般をも対象として開催した。例えば、小中学生を対象とする科学体験教室を毎年共催し、情報セキュリティに触れる場を設けたことは、本拠点が今後の生活に密着度が増すことが確実な電子社会と情報セキュリティに関する研究教育の成果を広く社会に還元することを強く意識していることの現れである。

また、これら企画に直接参加していなくても本拠点の成果を入手できるよう、主催会議の報告書、本拠点を紹介するリーフレットならびに成果報告書を制作・配布し、一部はWebpageを通じて公開した。また、本拠点の目的、構成、計画、成果、予定などを公表するためにWebpageを本拠点設置と同時に開設し、現在に至っている。中央大学がWebpageによるニュース配信を全学的に整備してからは、本拠点の動向が大学のトップニュースを飾ることも複数あり、効果的な情報発信がなされている。

これら、本拠点の積極的な情報発信の結果として、本拠点の成果が報道発表された事例もある。例えば、無線通信システムの信頼性向上に関する研究成果が日本SGI株式会社から2005年９月にプレスリリースされ、フジサンケイビジネスアイ、週刊アスキー、asahi.comなど新聞、雑誌、インターネットにて引用された。

7)拠点形成費等補助金の使途について（拠点形成のため効果的に使用されたか）

初年度は、主に拠点形成のための設備備品の購入を行なった。特に、３面没入型バーチャルリアリティ設備ChuoCAVEを導入した。このシステムは研究で得られたセキュリティ情報の可視化を行い、また、教育用にも使用され、多大なる貢献を果たし、今後もChuoCAVEは研究教育拠点としての設備の中核となることが期待されている。

次年度からは、情報セキュリティ分野における若手の研究者に育成に重点を置き、COE研究員、PDやRAを積極的に雇用する体制を取り、交付金額の約５割を若手の研究支援に使用し、若手の育成を行ってきた。その成果として、多くの優れた研究成果が得られたと言える。

世界水準の研究拠点として、毎年大規模な国際会議を開催し、研究発表や研究討論のために多くの外国人研究者を招聘し、国際的な研究交流を行ってきた。そのため、シンポジウム開催費や外国人研究者の招聘に関わる経費として交付金を使用した。また、若手研究者を中心として、国際的に通用する研究を行うために、海外出張のための費用にも使用している。

プログラム採択期間中に得られた成果は、随時、国際会議・研究論文として公表し、本拠点が主催したシンポジウムに関する内容は報告書として成果を公表してきた。そのための経費としても交付金を使用している。このように、拠点形成費等補助金は、拠点形成のために効果的に使用してきた。

②今後の展望

2003年度には、コンピュータセキュリティや脆弱性データベースなどの研究・指導者として土居範久教授を、2006年度には暗号技術全般にわたる研究・指導者として今井秀樹教授を中央大学に迎え、体制を強化した。さらに、2007年度に理工学研究科は博士後期課程『情報セキュリティ科学』専攻を新設し、また、2006年10月には「情報セキュリティ研究センター」を理工学研究所に設置し、本拠点において活躍されてきた教員を中心に、本拠点の研究教育体制を保ちながら、研究教育における成果をさらに発展する。特に、本学の強みである暗号の数学基礎理論に関する研究を継続発展すると同時に、人文・社会科学との連携をより深め、情報セキュリティ総合科学の構築と体系化に注力したい。

一方、情報セキュリティの幅広い人材育成については、2003年度採択の科学技術振興調整費「新興分野人材養成」拠点では情報セキュリティ管理者やネットワーク技術者を、2006年度採択の「先導的ITスペシャリスト育成推進プログラム」拠点では高度な実践的ICTスキルを備えた人材を育成し続ける。

③その他（世界的な研究教育拠点の形成が学内外に与えた影響度）

学内では、学長のリーダーシップの下での大学改革の中では、世界的教育研究拠点の形成とプロフェッショナルの育成において、基礎研究の充実を図る一方で、「安全・快適な暮らしの実現」をキーワードに、情報セキュリティのほか、環境、危機管理、国際関係を重点４分野として定め、新たな学際的総合科学の構築を目指している。一方、大学院においては、電子社会・情報セキュリティ副専攻、情報セキュリティ科学博士後期課程を始め、総合的な問題解決能力の育成を図るため、分野横断的なカリキュラムを開発し全学的な展開を志向している。

また、本拠点は、毎年「情報セキュリティ総合科学」に関するシンポジウムを開催し、情報セキュリティ人材育成拠点と共同公開講座を行い、本拠点の研究教育活動を通じで、社会的における情報セキュリティ技術に関する認知度と理解を高めるべく努めてきた。近年本学の情報セキュリティの研究教育拠点が社会一般に知られ、情報セキュリティ分野志願の高校生の中で、本学への進学希望者が急増している。さらに、本学は、地域貢献を重視しており、社団法人「学術・文化・産業ネットワーク多摩」の設立に参画したほか、2006年には文京区と教育の包括提携を行うなど、生涯学習講座や産学連携を通じた地域社会の活性化にも寄与している。

さらに、海外では、本学の楕円・超楕円暗号の研究拠点が評価され、Frey教授、Lang教授が率いるヨーロッパの研究グループとMurty教授が率いるカナダの研究グループなどの研究機関から、相次ぎ学術交流と共同研究が申し込まれた。本拠点は毎年国際会議を開催される以外に、海外研究拠点と定期的な国際交流を行ってきた。その結果、多数の新しい研究成果が生まれており、楕円・超楕円暗号の学問研究における新たな流れが作り出されている。

２１世紀ＣＯＥプログラム　平成１４年度採択拠点事業結果報告書

機　関　名	中央大学	拠点番号	C17
拠点のﾌﾟﾛｸﾞﾗﾑ名称	電子社会の信頼性向上と情報セキュリティ		

１．研究活動実績

①この拠点形成計画に関連した主な発表論文名・著書名【公表】

・事業推進担当者（拠点リーダーを含む）が事業実施期間中に既に発表したこの拠点形成計画に関連した主な論文等〔著書、公刊論文、学術雑誌、その他当該プログラムにおいて公刊したもの〕）
・本拠点形成計画の成果で、ディスカッション・ペーパー、Ｗｅｂ等の形式で公開されているものなど速報性のあるもの
※著者名（全員）、論文名、著書名、学会誌名、巻(号)、最初と最後の頁、発表年（西暦）の順に記入
波下線（＿＿＿）：拠点からコピーが提出されている論文
下線（＿＿＿）：拠点を形成する専攻等に所属し、拠点の研究活動に参加している博士課程後期学生

論文:

(1) 辻井重男, “電子社会を推進する情報セキュリティ総合科学のパラダイム,” 電子情報通信学会論文誌(A), vol.J87-A, no.6, pp.710－720, 2004.
(2) Shigeo Tsujii, Kohtaro Tadaki and Ryo Fujita, “Information Security as Interdisciplinary Science Based on Ethics,” Information Security and Cryptology - ICISC 2005 8th International Conference, pp.1－2, 2005.
(3) Shigeo Tsujii, Kohtaro Tadaki and Ryo Fujita, “Proposal for piece in hand matrix ver. 2: General Concept for enhancing security of multivariate public key cryptosystems,” Proceedings of International Workshop on Post-Quantum Cryptography (PQCrypto 2006), pp.23－26, 2006.
(4) Shigeo Tsujii, Kohtaro Tadaki and Ryou Fujita, “Proposal for piece in hand matrix; general concept for enhancing security of multivariate public key cryptosystems,” IEICE Transactions on Fundamentals, vol.E90-A, no.5, pp.992－999, 2007.
(5) 板倉征男, 長嶋登志夫, 辻井重男, “DNAバイオメトリックス本人認証方式の提案,” 情報処理学会論文誌, vol.43, no.8, pp.2394－2404, 2002.
(6) Yukio Itakura, Masaki Hashiyada, Toshio Nagashima and Shigeo Tsujii, “Proposal on personal identifiers generated from the STR Information of DNA,” International Journal of Information Security, vol.1, no.3, pp.149－160, 2002.
(7) Kazuto Matsuo, Jinhui Chao and Shigeo Tsujii, “An Improved baby step giant step algorithm for point couting of hyperelliptic curves over finite fields,” Algorithmic Number Theory, Springer-Verlag, Lecture Notes in Computer Science 2369, pp.461－474, 2002.
(8) Masaki Gonda, Kazuto Matsuo, Kazumaro Aoki, Jinhui Chao and Shigeo Tsujii, “Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.1, pp.89－96, 2005.
(9) Fumiyuki Momose and Jinhui Chao, “Scholten forms and elliptic/hyperelliptic curves with weak Weil restrictions,” Cryptology ePrint Archive: Report 2005/277, http://eprint.iacr.org/2005/277, 2005.
(10) Fumiyuki Momose and Jinhui Chao, “Classification of Weil restrictions obtained by (2,...,2) coverings of P^1,” Cryptology ePrint Archive: Report 2006/347, http://eprint.iacr.org/2006/347, 2006.
(11) Takao Asano, “An improved analysis of Goemans and Williamson's LP-relaxation for MAX SAT,” Theoretical Computer Science, vol.354, pp.339－353, 2006.
(12) Takao Asano and David P. Williamson, “Improved approximation algorithms for MAX SAT,” Journal of Algorithms, vol.42, pp.173－202, 2002.
(13) Mitsunori Makino, “Detection of edges and approximation of surfaces in the use of automatic differentiation in computer graphics,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E85-A, no.3, pp.558－565, 2002.
(14) Xiaoyi Cao, Mitsunori Makino, Hiroshi Shirai and Shoji Shinoda, “An interactively stereoscopic visual simulation on the CAVE for reliability and security of mobile communications systems,” Proceedings of Asia Simulation Conference 2005/The Sixth International Conference on System Simulation and Scientific Computing, vol.I, pp.461－465, 2005.
(15) 寺田真敏, 高田眞吾, 土居範久, “脆弱性対策情報データベースJVNの提案,” 情報処理学会論文誌, vol.46, no.5, pp.1256－1265, 2005.
(16) Toshihiko Koju, Shingo Takada and Norihisa Doi, “An efficient and generic reversible debugger using the virtual machine based approach,” Proceedings of ACM/USENIX Conference on Virtual Execution Environments, pp.79－88, 2005.
(17) Akio Tanaka, Keisuke Nakano, Masakazu Sengoku and Shoji Shinoda, “Analysis of communication traffic characteristics of a two-hop wireless network,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E85-A, no.7, pp.1436－1444, 2002.
(18) Ryuhei Funada, Hiroshi Harada and Shoji Shinoda, “Performance improvement of decision-directed OFDM channel estimation in a fast fading environment,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.87-A, no.8, pp.1994－2001, 2004.
(19) Kiyotaka Yamamura and Ryuji Kaneko, “Finding all solutions of piecewise-linear resistive circuits using the simplex method,” IEEE Transactions on Circuits and Systems I, vol.50, no.1, pp.160－165, 2003.

(20) Wataru Kuroki, Kiyotaka Yamamura and Shingo Furuki, “An efficient variable gain homotopy method using the SPICE-oriented approach,” IEEE Transactions on Circuits and Systems II, vol.54, no.7, 2007.
(21) Takakazu Sugiyama and Tomoya Yamada, “The permutation test in the canonical correlation analysis,” Computational Statistics ＆ Data Analysis, vol.50, pp.1－16, 2005.
(22) Michiyo Yamamoto, Takakazu Sugiyama, Hidetoshi Murakami and Fumitake Sakaori, “Correlation analysis of principal components from two populations,” Computational Statistics ＆ Data Analysis, vol.51, no.9, pp.4707－4716, 2007.
(23) Hiroshi Konno and Rei Yamamoto, “Minimal concave cost rebalance of a portfolio to the efficient frontier,” Mathematical Programming, Ser. B., vol.97, pp.571－585, 2003.
(24) Hiroshi Konno and Tomoyuki Koshizuka, “Mean-absolute deviation model,” IIE Transactions, vol.37, pp.893－900, 2005.
(25) 齊藤忠夫, “特集 新世代ネットワーク2 新世代ネットワークへの期待と課題,” 情報処理, vol.47, no.10, pp.1077－1082, 2006.
(26) 藤井光昭, 竹田裕一, 渡邊則生, 鎌倉俊成, 杉山高一, “暗号に用いる乱数の統計的仮説検定,” 日本統計学会誌, vol.35, no.2, pp.181－199, 2006.
(27) 鳥海重喜, 田口 東, “オブジェクトの空間的精度を第3次元とした3次元地理データベースの構築,” GIS－理論と応用－, vol.14, no.2, pp.19－30, 2006.
(28) 鳥海重喜, 田口 東, “個人情報保護を考慮した地理的情報の取り扱い,” 日本セキュリティ・マネジメント学会誌, vol.20, no.3, pp.3－12, 2007.
(29) Shigeki Toriumi, Hisao Endo and Keiko Imai, “Label size maximization for rectangular node labels,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E89-A, no.4, pp.1035－1041, 2006.
(30) Hiroshi Shirai and Hidenori Sekiguchi, “A simple crack depth estimation method from back scattering response,” IEEE Transaction on Instrumentation and Measurement, vol.53, no.4, pp.1249－1254, 2004.
(31) Shoji Mochizuki, Soichi Watanabe, Masao Taki, Yukio Yamanaka and Hiroshi Shirai, “A new iterative MoM/FDTD formulation for simulating human exposure to electromagnetic waves,” IEICE Transaction on Electronics, vol.E87-C, no.9, pp.1540－1547, 2004.
(32) Seigo Arita, Shinji Miura and Tsutomu Sekiguchi, “An addition algorithm on the Jacobian varieties of curves,” Journal of the Ramanujan Mathematical Society, vol.19, no.4, pp.235－251, 2004.
(33) Tsutomu Sekiguchi and Noriyuki Suwa, “A note on extensions of algebraic and formal groups V,” Japan Journal of Mathematics, vol.29, no.2, pp.221－284, 2003.
(34) 久米 均, “安全の管理－その特質と難しさ,” 特別企画 企業経営と安全の管理, 標準化と品質管理, vol.59, no.8, pp.4－10, 2006.
(35) Toshinari Kamakura, “Computational methods in survival analysis,” Handbook of Computational Statistics, Springer Berlin-Heidelberg New York, pp.767－785, 2004.
(36) Hideki Nagatsuka and Toshinari Kamakura, “Parameter estimation of the shape parameter of the Castillo-Hadi model,” Communications in Statistics Theory and Methods, vol.33, issue.1, pp.15－27, 2004.
(37) 中條武志, “人間行動に起因する事故の未然防止のための方法論の体系化,” 品質, vol.32, no.2, pp.225－237, 2002.
(38) 中條武志, “組織における不適切な人間行動とそのリスク評価,” 信頼性, vol.26, no.7, pp.627－635, 2004.
(39) 内田勝也, “情報セキュリティマネジメントからの個人認証システムの提案,” 日本セキュリティ・マネジメント学会誌, vol.20, no.1, pp.3－12, 2006.
(40) Steven J. van Enk and Osamu Hirota, “Entangled states of light and their robustness against photon absorption,” Physical Review A, vol.71, 62322, 2005.
(41) Kentaro Kato and Osamu Hirota,, “Square root measurement for quantum symmetric mixed state signals,” IEEE Transactions on Information Theory, vol.49, no.12, pp.3312－3317, 2003.
(42) 細野助博, “審議会型政策形成と情報公開の意義－「決定の質」の政策分析－,” 公共政策研究, vol.3, pp. 55－67, 2003.
(43) 伊理正夫, “空間情報の標準化の意義と現状,” 電子情報通信学会誌, pp.83－87, 2004.
(44) Yasutaka Ihara, “On the Euler-Kronecker constants of global fields and primes with small norms,” Algebraic Geometry and Number Theory, edited by Victor Ginzburg, Progress in Mathematics 253, Birkhäuser, pp. 407－451, 2006.
(45) Yasutaka Ihara, “The Euler-Kronecker invariants in various families of global fields,” Proceedings of Arithmetic, Geometry and Coding Theory 2005, edited by François Rodier and Serge Vladut, Société Mathématique de France, to appear.

著書:

(1) 辻井重男, 笠原正雄 (編著), “情報セキュリティ―暗号・認証・倫理まで,” 昭晃堂, 2003. (2) 土居範久(監修), 内田勝也 他 (編集), “情報セキュリティ事典,” 共立出版, 2003. (3) 辻井重男 (編著), “電子社会のパラダイム-その論理と倫理,” 新世社, 2002. (4) 辻井重男監修・執筆, “デジタル・フォレンジック事典,” デジタル・フォレンジック研究会編, 日科技連出版社, 2006. (5) 中條武志, 山田 秀 編著, “マネジメントシステムの審査・評価に携わる人のためのTQMの基本,” 日科技連出版社, 2006. (6) 堀部政男 編集, “インターネット社会と法 第2版,” 新世社, 2006. (7) 堀部政男 監修, “JIS Q 15001:2006個人情報保護マネジメントシステム要求事項の解説,” 日本規格協会, 2006. (8) 細野助博, “シチズン・リテラシー －社会をよりよくするために私たちにできること,” 教育出版, 2005. (9) 細野助博(編集代表 細野助博), “政策学入門,” 政策分析ネットワーク編, 2003. (10) Tadao Saito and Hiroshi Esaki, “Gigabit network,” IUS Press, 2003. (11) 内田勝也, 高橋正和, “有害プログラム,” 共立出版, 2004.

②国際会議等の開催状況【公表】

（事業実施期間中に開催した主な国際会議等の開催時期・場所、会議等の名称、参加人数（うち外国人参加者数）、主な招待講演者（３名程度））

(i) ″2003 International Symposium on Next Generation Cryptography and Related Mathematics ″
期　日:2003.02.11-13　　参加者数:130(8)
会　場:International Conference Hall, Ichigaya Campus, Chuo University
主な招待講演者:　Manindra Agrawal (Indian Institute of Technology Kanpur, India)
Kumar Murty (Toronto University, Canada)
Pierrick Gaudry (École Polytechnique, France)

(ii) ″ 2003 Workshop on Cryptography and Related Mathematics ″
期　日:2003.09.09-11　　参加者数:120(8)
会　場:中央大学後楽園キャンパス3号館14階大会議室
主な招待講演者:　Ran Canetti (IBM Research)
Qing Liu (CNRS)
Robert Pollack (University of Chicago)

(iii) ″ 2004 Workshop on Cryptography and Related Mathematics ″
期　日:2004.08.06-08　　参加者数:100(9)
会　場:中央大学後楽園キャンパス3号館小ホール
主な招待講演者:　Rene Schoof (University of Rome ″Tor Vergata″)
Steven Galbraith (Royal Holloway, University of London)
Amit Sahai (Princeton University)

(iv) ″ Workshop On GrÖbner basis and Application to Cryptography ″
期　日:2004.12.11　　参加者数:62(1)
会　場:中央大学後楽園キャンパス3号館6階 3609号室
主な招待講演者:Gwénolé Ars　(Université de Rennes 1)

(v) ″ 2005 Workshop on Cryptography and Related Mathematics ″
期　日:2005.08.08-10　　参加者数:110(10)
会　場:中央大学後楽園キャンパス3号館小ホール
主な招待講演者:　Gerhard Frey (Institute for Experimental Mathematics, University of Duisburg-Essen)
Rene Schoof (University of Rome ``Tor Vergata″)
Kumar Murty (University of Toronto)

(vi) ″ Workshop on Quantum Communication Theory and the Related Topics ″
期　日:2005.08.22-23　　参加者数:30(3)
会　場:Research Center for Quantum Communications, Room Number 210, 2nd floor, Research & Management Headquarters, Tamagawa University, Machida, Tokyo
主な招待講演者:　V.P.Belavkin (University of Nottingham, UK)
E.Corndorf (Northwestern University, USA)
Y.L.Hsu (Chung Yuan Christian University, TAIWAN)

(vii) ″ Symposium on Reliable and Robust Wireless Networks and EMC ″
期　日:2005.09.10　　参加者数:45(2)
会　場:Chuo University, Korakuen Campus, Room 3300
主な招待講演者:　Mario Gerla (UCLA, USA)
Kenichi Mase (Niigata University, Japan),
Mitsutoshi Hatori (Chuo University)

(viii) ″ Symposium on Quantum Cryptography by Optical Communications ″
期　日:2005.11.28-29　　参加者数:120(5)
会　場:中央大学後楽園キャンパス3号館14階大会議室
主な招待講演者:　H.P.Yuen (Northwestern University USA)
P.Kumar (Northwestern University, USA)
H.E.Brandt (U.S. Army Research Laboratory, USA)

(ix) ″ Symposium on Algebraic Curves ″
期　日:2005.12.19-22　　参加者数:60(4)
会　場:中央大学後楽園キャンパス3号館11階31112号室
主な招待講演者:　C.Carvalho (Brazil)
M.Coppens (Bergium)
A.Garcia (Brazil)

(x) ″ Workshop on Arithmetic Geometry, Related Area and Applications ″
期　日:2006.04.06-04.07　　参加者数:40(3)
会　場:中央大学後楽園キャンパス3号館3階3300号室
主な招待講演者:　Barry Green (Stellenbosch 大学)
Michel Matignon (Bordeaux 大学)
Mohamed Saidi (Exeter 大学/数理解析研究所)

(xi) ″ Workshop on Applications of Body Area Radiowaves ″
期　日:2006.08.01　　参加者数:100(20)
会　場:中央大学後楽園キャンパス1号館3階1225号室
主な招待講演者:　Chung-Kwang Chou (Motorola, USA)
Kenneth R. Foster (Univ. of Pennsylvania, USA)
Jean-Charles Bolomey (Supelec, France)

(xii) ″ 2006 Workshop on Cryptography and Related Mathematics ″
期　日:2006.08.01-08.03　　参加者数:100(14)
会　場:中央大学後楽園キャンパス3号館小ホール
主な招待講演者:　Brian Conrad (University of Michigan)
Gerard van der Geer (University of Amsterdam)
Olivier Pereira (Universite Catholique de Louvain)

２．教育活動実績【公表】

博士課程等若手研究者の人材育成プログラムなど特色ある教育取組等についての、各取組の対象（選抜するものであればその方法を含む）、実施時期、具体的内容

（１）　若手研究員及びＰＤ（ポストドクター）の採用（履歴書・業績書、面接による）

加藤研太郎、志村真帆呂、竹田　裕一、只木孝太郎、津田　美幸、土屋　和由、谷戸　光昭、関口　秀紀　以上8名

（２）　ＲＡ（リサーチ アシスタント）の採用（面接による）

ⅰ．2002年度の採用（以下7名）

遠藤章次、小澤信太郎、酒折文武、土屋和由、谷戸光昭、船田龍平、長塚豪己

ⅱ．2003年度の採用（以下10名）

李聖鍵、相良直哉、鈴木則充、関口秀紀、曹暁逸、土屋和由、鳥海重喜、長塚豪己、船田龍平、堀川大介

ⅲ．2004年度の採用（以下13名）

李聖鍵、飯島努、宇津木修一、相良直哉、示沢寿之、曹暁逸、鳥海重喜、新妻康弘、原口幸、船田龍平、前田康智、望月章志、山口鉄平

ⅳ．2005年度の採用（以下11名）

李潤喆、飯島努、宇津木修一、尾崎永児、相良直哉、曹暁逸、鳥海重喜、山口鉄平、新妻康弘、原口幸、示沢寿之

ⅴ．2006年度の採用（以下9名）

李潤喆、飯島努、宇津木修一、鳥海重喜、山口鉄平、尾崎永児、前田康智、黒木渉、高島愛

（３）　若手研究者・後期課程(事業推進担当者の所属する専攻)学生の学会発表状況

国内外の学会で若手研究者や後期課程の学生が発表する際に旅費を支給して、発表の機会を促進した。

ⅰ．2002年度　　－　　後期課程学生:国内7名、外国16名

ⅱ．2003年度 COE研究員の学会発表状況：国内2名、外国1名　後期課程:学生国内13名、外国5名

ⅲ．2004年度 COE研究員の学会発表状況：国内9名、外国2名　後期課程:学生国内6名、外国10名

ⅳ．2005年度 COE研究員の学会発表状況：国内3名、外国4名　後期課程:学生国内9名、外国6名

ⅴ．2006年度 COE研究員の学会発表状況：国内6名、外国3名　後期課程:学生国内10名、外国7名

（４）　研究発表会の開催若手研究者を主体とする研究発表会を、下記のように開催した。

ⅰ．2003年3月10日 RA（Research Assistant）による研究発表

ⅱ．2003年7月29日 COE研究員による発表

ⅲ．2003年12月8～12日　RAによる研究発表会（ポスターセッション形式により、ＲＡが研究成果を発表。）

ⅳ．2004年12月8日　RAによる研究発表会（ポスターセッション形式により、ＲＡが研究成果を発表。）

ⅴ．2005年12月7日 RAによる研究発表会（ポスターセッション形式により、ＲＡが研究成果を発表。）

ⅵ．2006年12月6日 RAによる研究発表会（ポスターセッション形式により、ＲＡが研究成果を発表。）

（５）　副専攻及び特別研修コースの開催

2003年度から理工学研究科に電子社会・情報セキュリティ副専攻を設置し、主専攻に加えて副専攻の科目を履修し必要な単位修得し、リサーチペーパーの審査に合格すれば副専攻修了書を授与している。また。同じく2003年度から文部科学省の科学技術振興調整費「情報セキュリティ・情報保証　人材育成拠点」を受けて特別研修コースを開催している。

＜副専攻＞

電子社会・情報セキュリティ副専攻：2003年度～2006年度修了者累計＝36名

＜人材育成拠点＞

・実践講座（Windowsセキュリティ）：2003年度～2006年度修了者累計＝163名

・実践講座（UNIXセキュリティ）：2004年度～2006年度修了者累計＝127名

・実践講座（セキュアプログラミング）：2004年度～2006年度修了者累計＝43名

・実践講座（ｲﾝｼﾃﾞﾝﾄﾚｽﾎﾟﾝｽ&情報法科学）：2005年度～2006年度修了者累計＝44名

・情報セキュリティマネジメント講座：2004年度～2006年度修了者累計＝77名

・公開講座：2004年度～2006年度修了者累計＝214名

・ＳＡＮＳ講座：2003年度～2006年度修了者累計＝49名

・脆弱性ＤＢ構築を通した高度技術者の育成：2004年度～2006年度修了者累計＝9名　　人材育成拠点　合計＝762名

（６）　ＲＡ経験者の博士号取得

2002年度の取得者:谷戸光昭、酒折文武の2名。

2003年度の取得者:遠藤章次、土屋和由、関口秀紀、長塚豪己の4名。

2004年度の取得者:李聖鍵、船田龍平、望月章志の3名。

2005年度の取得者:相良直哉、示沢寿之の2名。

2006年度の取得者:飯島努、鳥海重喜、新妻康弘、原口幸の4名。

機関名：　中央大学　　拠点番号：　Ｃ１７

２１世紀ＣＯＥプログラム委員会における事後評価結果

（総括評価）

設定された目的は概ね達成され、期待どおりの成果があった

（コメント）

拠点形成計画全体について、本ＣＯＥは情報セキュリティという現代社会に大きなインパクトを与える項目に焦点を当て、学問・技術・ビジネス・制度にまたがる教育研究を推進するユニークなプログラムであり、電子社会・情報セキュリティ副専攻の設立、情報セキュリティ科学専攻の設立、研究開発機構との連携、外国大学の拠点との交流、国際シンポジウムの開催など、拠点としての活動を積極的に推進し、本プログラム終了後も継続できる体制を構築したことを評価する。

人材育成面では、事業推進担当者が指導教員である博士課程入学者数が少なく、高度な情報セキュリティ技術を担う若い研究者の育成がまだ十分でない点が今後の課題である。

研究活動面について、本プログラムの重要課題として超楕円暗号理論や量子暗号理論については速報誌に論文が掲載されるなど、積極的に推進しているが、理論研究におけるフルペーパーの発表がまだ十分でないと思われ、今後一層の成果発表が期待される。

また、中間評価のコメントで指摘されている、情報セキュリティの総合的な取り組みについては、研究分野を３つの階層に整理し、階層間のコミュニケーションを図る施策を採りつつあるが、階層をまたがる技術やプロトコル、標準化、などの具体的成果が望まれる。