私の研究活動

2026年10月20日

経営学部　永田清

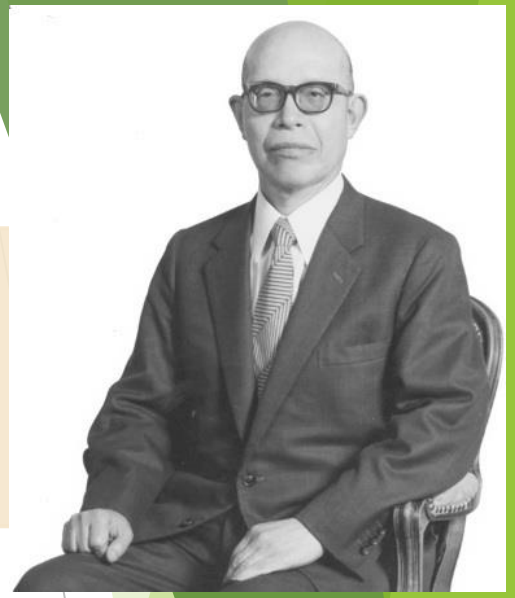
研究・活動の流れ（数学・応用数学)

上智大学数学科　修士課程　　博士課程満期退学

	1976年	1980年	1982年	1986年	1988年	1990年	1993年	1996年
一般	**RSA暗号方式 (1977)**		**楕円曲線暗号 (1985年)**				**The Z_4 linearity of Kerdock, Preparata, Goethals and related codes**	
勉強・研究	非可換環論ゼミ	整数論(代数体上の整数基底，類体論，L関数) カテゴリー論		AMSReviewer Kumasi大学発表 (Galois理論基礎)	PC操作 (MS-DOS，アプリ等)	Fortran 表計算ソフト	PC操作， 整数論， 誤り訂正符号 マルチメディア表現	
生活	大学生	修士	博士学生	青年海外協力隊 (ガーナ) クマシ大学学生	中高非常勤就活	私立 栄光学園	非常勤講師	大東文化大学 経済学部専任講師

	1997年	1999年	2005年	2009年	2016年	2019年	2024年	2026年
一般	**Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer(by Shor, 1997)**					**Post-Quantum Cryptography(NIST)**		
勉強・研究	暗号理論(楕円曲線，超楕円曲線生成) 耐量子乱数生成，ゼロ知識証明 誤り訂正符号(Self-Dual Code)			誤り訂正符号 (Self-Dual Code over Z/psZ)		Python，Javaアプリケーション 耐量子暗号 Self-Dual Codeとカテゴリー論(森田理論)		
生活	経済学助教授	経営学部教授 中央大学社会人大学院		博士学位 (工学，中央大学)	学科主任，内部監査委員長， ハラスメント調査委員長， 大学基準協会委員，長期海外研究期間(2013年～2014年)		情報センター所長 学部長，図書館長， サバティカル(2024年度) 経営研究所長	

研究・活動の流れ（数学・応用数学)

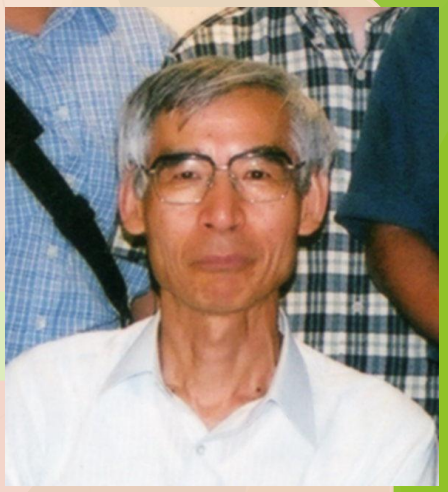


上智大学数学科

- 4年森田ゼミ
  - 森田紀一(1915-1995)
  - 「森田同値が数学を変えた──天才数学者・森田紀一の生涯と功績」, https://youtu.be/Ebz2SMkoB8o
  - 非可換環論(Rings and Homology)
  - カテゴリー論

修士課程

- 和田秀男ゼミ
  - 和田秀男(1940年12月26日 - 2012年1月7日)
  - 「2次体上の純3次拡大における相対整数基底と相対判別式」
  - 和田先生の結果を一般化



博士課程

- 和田秀男ゼミ
  - 類体論
  - ArtinのL-関数
  - “On Bases of Purely Cubic Fields over Quadratic Fields”, *Tokyo Journal of Mathematics* Vol.7 No.2, pp. 121-131, 1985
  - “Artin's L-functions and Gassmann Equivalence”, Tokyo Journal of Mathematics Vol.9 No.2, pp.357-364, 1986

研究・活動の流れ（数学・応用数学)

1993年4月～1996年3月
非常勤講師

- 和田秀男研究室
- Philippine大学からの留学生
  Fidel Nemenzo氏

1996年4月～1999年3月
専任講師

- On some type of integers and their experimental properties, 日本数学会発表
- “公開鍵方式における暗号理論と応用”，大東文化大学紀要第37号〈社会科学〉

1999年4月～2007年3月

助教授，准教授，教授

- “Secure Socket Layer(SSL)における情報保護の数理”，“ゼロ知識対話証明”，“暗号技術の評価及び評価機関”，“Hash関数と擬似乱数生成” 等
- “虚数乗法をもつ楕円曲線とj-不変量について”，大東文化大学紀要41号〈自然科学〉
- “超楕円曲線におけるWeil数について”，
  経営論集第9号，大東文化大学経営学会

研究・活動の流れ（数学・応用数学)

2007年4月～
2009年3月

- 和田秀男研究室
- Philippine大学数学科Fidel Nemenzo氏
- 誤り訂正符号(Mass Formula of Self-dual Code)
  - “On Construction of self-dual code over Z/p^sZ”, Mathematical Society of the Philippines 2007 Convention, Tagbilaran City in Bohol
  - “Constructive Algorithm of Self-Dual Error-Correcting Codes”, Proceeding of the 11th International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2008, Pamporovo in Bulgaria
  - “The number of self-dual codes over Z_{p^3}”, *Journal of Designs, Codes and Cryptography*, Vol. 50, NO. 3, 2009
  - “On Self-Dual Codes over Z_{16}”, Proceeding of the 18th Symposium on Applied algebra, Algebraic Algorithms, and Error Correcting Coding, AAECC-18, Taragona, Spain,2009

研究・活動の流れ（数学・応用数学)

2007年4月～
2009年3月

- 中央大学大学院　辻井重男　研究室, 今井 秀樹
  - 辻井重男(1933年9月13日-)
    情報工学者,工学博士（東京工業大学・論文博士・学位論文「PCM通信に対する最適波形とその伝送に関する研究」. 東京工業大学名誉教授, 元一般財団法人マルチメディア振興センター理事長, 一般社団法人セキュアIoTプラットフォーム協議会理事長, 元電子情報通信学会会長, IEEEライフフェロー, 2002年日本セキュリティ・マネジメント学会会長, 2003年日本学術会議会員, 2004年情報セキュリティ大学院大学学長, 2009年放送倫理・番組向上機構評議員, 2010年マルチメディア振興センター理事長,放送セキュリティセンター理事長, **2009年瑞宝中綬章**
  - 今井秀樹(1943年－)
    暗号研究者. Ph.D.(東京大学, 電気工学), 同年から1992年まで横浜国立大学、東京大学名誉教授. 1998年電子情報通信学会基礎・境界ソサイエティ会長産業技術総合研究所(AIST)情報セキュリティ研究センター(RCIS)研究センター長. **2024年秋叙勲 瑞宝中綬章**
- 工学博士号(中央大学)
  - 「Construction of Self-Dual Error Correcting Codes over Finite Integer Ring Modulo p^s and their Mass Formulae」

研究・活動の流れ（数学・応用数学)

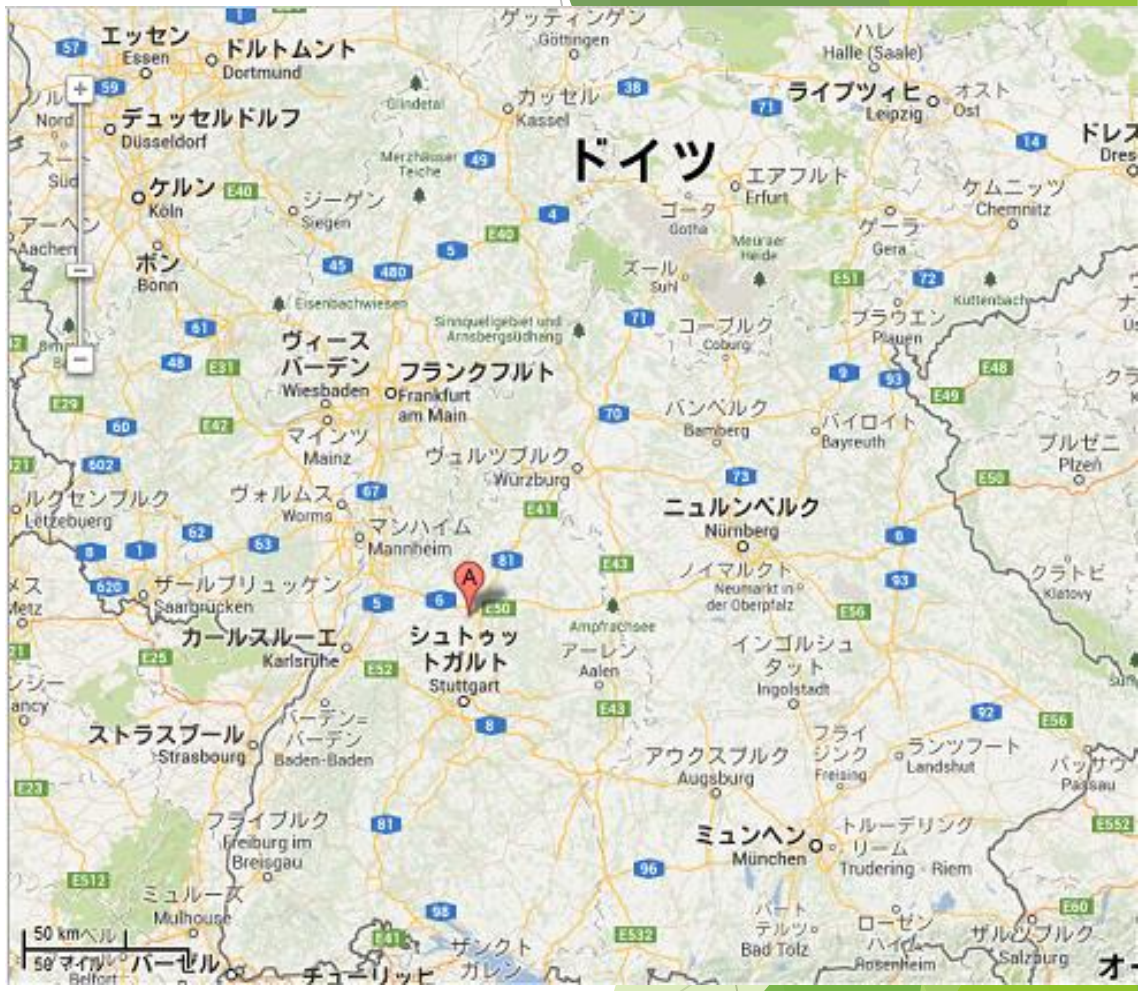
2009年4月～

2023年3月

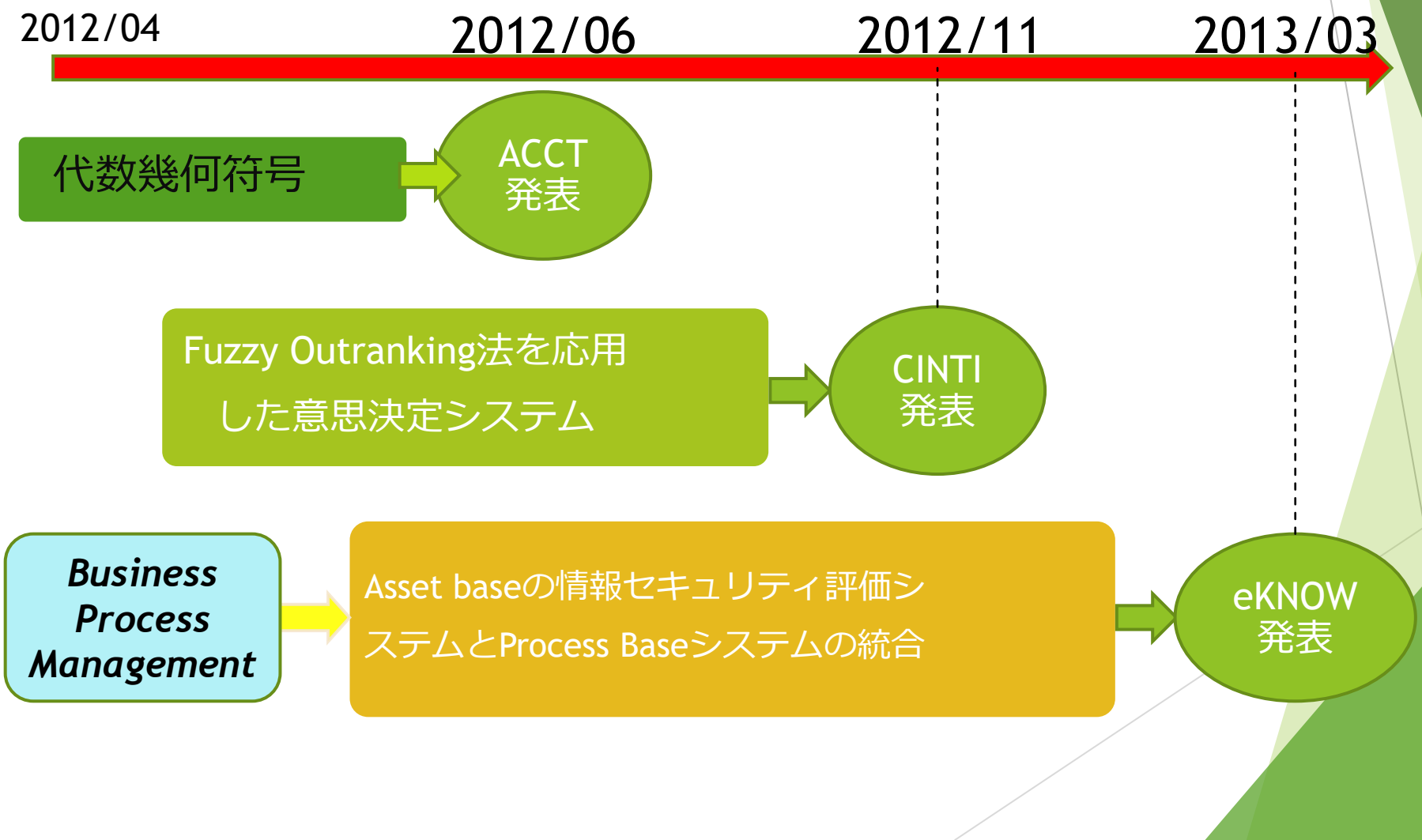
- “A Family of Codes on Projective Surface”, Proceeding of the 13th International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2012, Albena, Bulgaria
- “Mass formula and construction of self-dual codes over Z_{2^s}”, *Journal of Designs, Codes and Cryptography*, Vol.67, NO. 3, 2013
- “Calculation of Minimum Product Distance of Lattice Code”, *Journal of Information Engineering Express*, Vol. 1, No. 1, 2015
- “Some Properties of Binary Gray Code”, Proceedings of International Conference on Computer Application Technologies, Aug. 31-Sep. 2, 2015
- “On Post-Quantum Cryptography with Error-Correcting Code”, The 1st International Conference on ICT Application Research (IAR 2023)

長期海外期間

- 2012年4月1日～2013年3月31日
- ドイツ南西部
  - **ハイルブロン**
    （Heilbronn; Baden-Wurttemberg州北部）
  - 人口約12万人
  - 面積約100㎢



研究の時系列


2012/04
2012/06
2012/11
2013/03
代数幾何符号
ACCT
発表
Fuzzy Outranking法を応用
した意思決定システム
CINTI
発表
Business
Process
Management
Asset baseの情報セキュリティ評価シ
ステムとProcess Baseシステムの統合
eKNOW
発表

研究・活動の流れ（数学・応用数学)

2023年4月～

2026年3月

- “Survey on PQCC with Self Dual Code over Integer Modulo Ring”, Proceedings of the International Conference on ICT Application Research, 2024/11
- “Python によるZ_8上の自己双対誤り訂正符号の生成”, 第18回 国際ICT利用研究学会 研究会，旧大連航路上屋（北九州市門司区）, 2025年7月
- “Possibility of Applying Self-Dual Code over Integer Modulo Ring as PQCC”, Proceedings of the International Conference on ICT Application Research, 2025/11
- “Self-dual Code based PQCC and Critical Issues for Implementation”, Proceedings of The 4th International Conference on ICT Application Research, Iloilo, Philippines, 2026/3/31

2024年4月1日～2025年3月31日 特別研究期間制度取得

- 申請書における研究課題（以下の各課題を並行して研究する）
  - 整数の剰余環上における誤り訂正符号生成手法の耐量子暗号への応用
  - 工学オントロジーを用いた多言語対応情報セキュリティポリシー作成システムの研究と開発
  - 情報セキュリティe-Learningシステムへの多言語自然言語処理の組込み

7月29日～8月26日
Philippine University, Diliman校, Manila, Philippine

- 整数の剰余環上における誤り訂正符号生成手法の応用
- Fidel Nemenzo教授との共同研究
- 耐量子暗号(PQCC：Post Quantum Computer Cryptography)への適用可能性に関する研究
- 教員及び大学院生との研究会に5回参加・発表

10月28日～11月12日
Indraprastha Institute of Information Technology(IIIT-Delhi), New Delhi, India

- IIIT-Delhi数学科のAnuradha Sharma教授との共同研究
- 一般Galois環上の誤り訂正符号の実用化に関する研究
- 教員及び大学院生との研究会に3回参加・発表

Indraprastha Institute of Information Technology(IIIT-Delhi)



Indraprastha Institute of Information Technology, Delhi

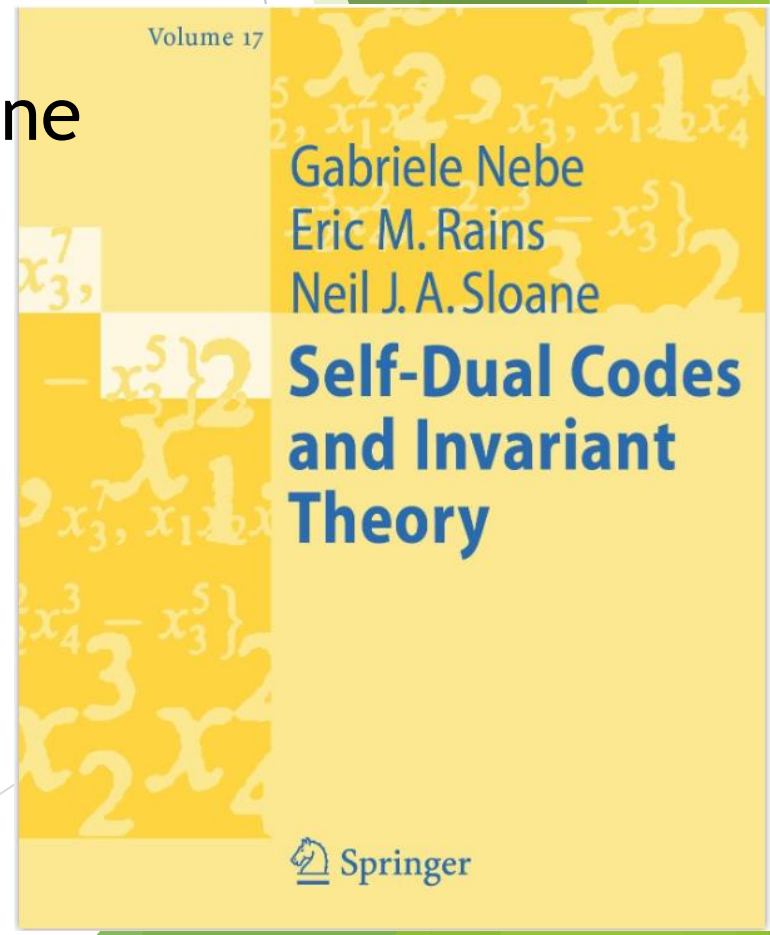


The campus in 2024

Other name	IIIT-D, IIIT Delhi
Type	State university
Established	2008; 17 years ago
Chairperson	Rajesh Srivastava
Chancellor	Lieutenant Governor of Delhi
Director	Ranjan Bose
Address	Okhla Industrial Estate, Phase III, New Delhi, 110020, India 28°32′40″N 77°16′21″E
Campus	Urban, 25 acres (10 ha)
Language	English
Colours	
Website	www.iiitd.ac.in

Text Book

- Self-Dual Codes and Invariant Theory
  (Algorithms and Computation in Mathematics Book 17)
  (English Edition) 2006th 版, Kindle版
- (著) Gabriele Nebe, Eric M. Rains, Neil J. A. Sloane
- Chapter 13 Quantum Codes
  - 13.1 Definitions
  - 13.2 **Additive and symplectic quantum codes**
  - 13.3 Hamming weight enumerators
  - 13.4…



研究・活動の流れ（情報教育・意識調査分析）

	1986年	1988年	1990年	1993年	1996年	1999年	2000年	2006年	2009年
一般			**Windows 3.0**	**インターネットの商用利用 NII構想，GII構想，WWW開発**		**e-Japan構想**		**i-Japan構想**	
勉強・研究	英語の授業 (数学)	英語の授業 (Colleage Mathmatics)		コンピュータ意識調査， 統計分析(因子分析，仮説検定等) SPSS		情報セキュリティ意識調査 情報倫理教材の多言語化 アジア各国の情報倫理意識調査			
生活	青年海外協力隊 (ガーナ) クマシ大学学生	中高非常勤 就活 上智大学比較文化学科非常勤講師	私立栄光学園	非常勤講師	大東文化大学経済学部専任講師	経済学准教授 経営学部准教授		経営学部教授 中央大学社会人大学院	

	2009年	2016年	2019年	2026年
一般	**u-Japan構想(2010年)**			
勉強・研究	E-learning System MBTI Learning styles(Kolb, Felder-Silverman)		情報セキュリティ意識とLearning stylesの関係 E-Learning Javaアプリケーション Ontology理論	
生活	博士学位 (工学，中央大学)	長期海外研究期間(2013年～2014年)	学科主任，内部監査委員長， ハラスメント調査委員長， 大学基準協会委員，長期海外研究期間(2013年～2014年)	情報センター所長 学部長，図書館長， サバティカル(2024年度) 経営研究所長

研究・活動の流れ（情報教育・意識調査分析）

1986年4月～1988年3月
青年海外協力隊
西アフリカ・ガーナ
理数科教師

- Nkawkaw Secondary School
- American Mathematicians Society(AMS)の Reviewerとして3，4本の論文にレビューを書く
- クマシ大学数学教室の研究生
- 数学教室でガロア理論の基礎の講義



研究・活動の流れ（情報教育・意識調査分析）

1995年4月～

2010年3月

- “情報基礎教育に関する学習意識”, 教育システム情報学会第20回全国大会論文集, 1995年8月
- “経験と所有が及ぼす対コンピュータ意識の変化”, 平成7年度情報処理教育研究集会講演論文集, 1995年12月
- “情報処理教育が及ぼす対コンピュータ意識の変化”, 平成9年度情報処理教育研究集会講演論文集, 1997年10月
- コンピュータネットワーク不安意識 -電子メール利用における場合-, 平成10年度情報処理教育研究集会講演論文集, 1998年10月
- “メディア嗜好によるグループ化とコンピュータセキュリティ意識”, 平成11年度情報処理教育研究集会講演論文集, 1999年11月,
- “学生のコンピュータセキュリティ意識とメディア嗜好の関係”, 平成12年度情報処理教育研究集会講演論文集, 2000年12月
- “情報倫理教材の多言語化とその必要性－アジア諸国における情報倫理教育の現状と課題－”, 教育システム情報学会第32回全国大会講演論文集，2007年9月
- “情報倫理教育教材の多言語化とアジアの現状”, 平成19年度情報教育研究集会講演論文集, 2007年11月
- “アジア各国における学生の情報倫理教育と意識および関連法制度”, 平成21年度情報教育研究集会講演論文集，(平成21年度情報教育研究集会最優秀論文賞), 2009年11月

研究・活動の流れ（情報教育・意識調査分析）

2010年4月～

2018年3月

- “中国語圏における学生の情報倫理教育と意識”,教育システム情報学会第35回全国大会講演論文集, 2010年8月
- “アジア各国からの留学生に対する情報倫理教育システム”,大学ITC推進協議会2011年次大会講演論文集, 2011年12月
- “Multilingual E-Learning System for Information Security Education with Users' Consciousness”, *Advances in Web-Based Learning - ICWL2014, Lecture Notes in Computer Science 8613*, Springer, Tallin, Estonia,2014/8
- “E-Learning Systems based on User's Consciousness and Characteristic”, Proceedings of International Conference on Computer Application Technologies, 2015/8
- “Learning Style and Consciousness Factors in E-Learning System on Information Security”, Teaching and Learning in a Digital World, Advances in Intelligent Systems and Computing, Vol.715, Springer, 2017/9

研究・活動の流れ（情報教育・意識調査分析)

2018年4月～

2026年3月

- “Trial for E-Learning System on Information Security Incorporate with”, *International Journal of Engineering Pedagogy (iJEP)*, Vol. 8, No. 3, 2018/5
- “Ontological Approach for Information Security e-Learning System”, International Congress on Education and Learning (ICEL - 2023), 24th -25th, Milan, Italy, 2023/10
- “Learning Style Recognition in relation with MBTI and FSLSM”, Proceedings of the International Conference on ICT Application Research, 2024/11
- “Learning Styles and Ontological Approach for Information Security e-Learning System”, In *Futureproofing Engineering Education for Global Responsibility, Lecture Notes in Networks and Systems, vol 1261*. Springer, 2025/3
- “Data Science Education in Japan -History and Current Status-”, Proceedings of the 3rd International Conference on ICT Application Research, 2025/11

2024年9月23日～9月27日
Tallinn University of Technology，Estonia
International Conference on Learning ICL2024

- “Learning Styles and Ontological Approach for Information Security e-Learning System”の発表
- 論文：Futureproofing Engineering Education for Global Responsibility. (ICL 2024), Lecture Notes in Networks and Systems, Springer, Cham. Vol 1261,207-218

研究・活動の流れ（Fuzzy理論・システム構築）

一般	1950年	1964年	1965年	1992年	1995年	2000年
研究	Theory of Reproducing Kernel by Aronszajn	Theoretical foundations of the potential function method in pattern recognition learning by Aizerman, M. A.	Fuzzy理論 by L. A. Zadeh	Balanced Scorecards, by Robert S. Kaplan and David Norton	BS7799	OCTAVE^{SM}(Operationally Critical Threat, Asset, and Vulnerability Evaluation System)

1996年　1999年 2000年　2005年　2009年　2016年　2019年　2026年

一般	**Fuzzy Regression Analysis by Neural Networks, 1996, by Ishibuchi, et al.**				**教育情報セキュリティポリシーに関するガイドライン(2017年)　文部科学省**	
勉強・研究	情報セキュリティ評価システム Fuzzy理論(Fuzzy Inference，etc.) 重要資産リスク評価，BSC， リスク低減システム			Fuzzy理論(Fuzzy Clustering，Fuzzy Outranking) 意思決定理論，WebSite評価システム		Fuzzy回帰分析 Kernal 法 情報セキュリティポリシー Neural Networkを使ったFuzzy回帰モデル
生活	大東文化大学経済学部専任講師	経済学准教授 経営学部准教授	経営学部教授 中央大学社会人大学院	博士学位 (工学， 中央大学)	学科主任， 内部監査委員長， ハラスメント調査委員長， 大学基準協会委員 長期海外研究期間(2013年～2014年)	情報センター所長， 学部長， 学科主任， 図書館長， サバティカル(2024年度) 経営研究所長

研究・活動の流れ（Fuzzy理論・システム構築)

2003年4月～

2009年3月

- “情報的側面からの企業評価指標”, Research Paper No.J-45, Institute of Business Research Daito Bunka University, 2003
- “企業評価の現状と動向”, Research Papers No.J-48, Institute of Business Research Daito Bunka University, 2006
- “Behavior Analysis of Passengers for East Japan Railway Company-Application of Modified Structural Modeling Method-”,Proceedings of the 7th APIEMS Conference, 2006, 17-20 December 2006, Bangkok, Thailand
- “Integrating Modified Structural Modeling Method with an Information Security Evaluation System”, Proceedings of the 8th APIEMS Conference 2007, 9-12 December 2007, Kaohsiung, Taiwan
- “Modified Structural Modeling Method and Its Application -Behavior Analysis of Passengers for East Japan Railway Company-”, *Journal of Industrial Engineering & Management Systems*, published by Korean Institute of Industrial Engineers(KIIE), Vol. 7, NO. 3, 2008
- “Risk Evaluation for Critical Assets with Fuzzy Inference Mechanism in an Information Evaluation System”, Proceedings of the 9th APIEMS Conference 3-5 December 2008, Bali, Indonesia

研究・活動の流れ（Fuzzy理論・システム構築)

2009年4月～

2012年3月

- “Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking”, Proceedings of the 9th International Conference on Intelligent Systems Design and Applications, 2009/11, Pisa, Italy
- “User Oriented Information Quality Evaluation System with Fuzzy Measures -Application for Website’s Search Engines-”, Proceedings of the 10th APIEMS Conference 2009/12/14-16, Kokura, Japan
- “Methodology for Evaluation of Linked Multidimensional Measurement System with Balanced Scorecard”, Proceedings of Information Processing and Management of Uncertainty, IPMU 2010, Part II, CCIS 81, Springer-Verlag Berlin Heidelberg, 2010/7
- “Risk Scoring Method on Business Information Management System”, Proceedings of the 11th APIEMS Conference, 2010/12, Melaka, Malaysia
- “A Study on User Evaluation System for E-Business Website”, Proceedings of the 11th APIEMS Conference 2010/12, 7-10, Melaka, Malaysia
- “On Clustering of Risk Mitigation Controls”, Proceedings of The 14-th International Conference on Network-Based Information Systems(NBiS-2011), 2011/9, Tirana, Albania
- “A Study on E-Business Website Evaluation Formula with Variables of Information Quality Score”, Proceedings of the 12th APIEMS Conference 2011/10, Beijing, China

研究・活動の流れ（Fuzzy理論・システム構築)

2012年4月～

2017年3月

- “Construction of Effective Database System for Information Risk Mitigation”, *Security Enhanced Application for Information Systems*, INTECH Open Access Publisher, 2012/05/30
- “Multi-attribute Decision Making Based on Fuzzy Outranking”, 13th IEEE International Symposium on Computational Intelligence and Informatics, 2012/11/20-22, Budapest, Hungary
- “Security of Information System in View of Business Continuity Management”, The Fifth International Conference on Information, Process, and Knowledge Management, 2013/2
- “Information Security Mitigation Controls with Fuzzy Linguistic Order”, dings of the 14th APIEMS Conference 2013, 2013/12/3-6, Cebu, Philippines
- “Evaluation Method of Information Value Applying for Website”, Proceedings of the 15th APIEMS Conference, 2014/10/12-15, Jeju, Korea
- “A Decision Making System for Cloud Computing Adoption Focused on Security Issues”, Proceedings of the 16th APIEMS Conference , 2015/12/8-11, HoChi Minh City, Vietnam
- “Prediction Model with Interval Data -Toward Practical Applications-”, Information Processing and Management of Uncertainty in Knowledge-Based Systems, Communications in Computer and Information Science, Springer, 2016/6

研究・活動の流れ（Fuzzy理論・システム構築)

2017年4月～

2020年3月

- “Decision Making by a Fuzzy Regression Model with Modified Kernel”, Proceedings of The Seventh International Conference on Advances in Information Mining and Management, Best Paper Award, Venice, Italy, 2017/6/
- “A Decision Support System for Cloud Computing Adoption”, Proceedings of the APIEMS Conference, 2017/12/2-6, Yogyakarta, Indonesia
- “Fuzzy Regression Model with Modified Kernel and its Application to a Set of Real Data”, *International Journal on Advances in Software, vol. 11, no. 1 & 2*, published by IARIA, 2018/6
- “Performance Evaluation of Web Information Retrieval Systems”, IAET International Conference on Big Data Management, System Engineering, Information Technology, Networking & Applied Sciences (BSIN), Budapest, Hungary, 2019/8
- “Construction of Support System for Information Security Policy”, Proceedings of APIEMS Conference, 2019/12/2-5, Kanazawa, Japan
- “Website evaluation using cluster structures”, *Journal of Advances in Technology and Engineering Research*, 5(1), 2019

研究・活動の流れ（Fuzzy理論・システム構築)

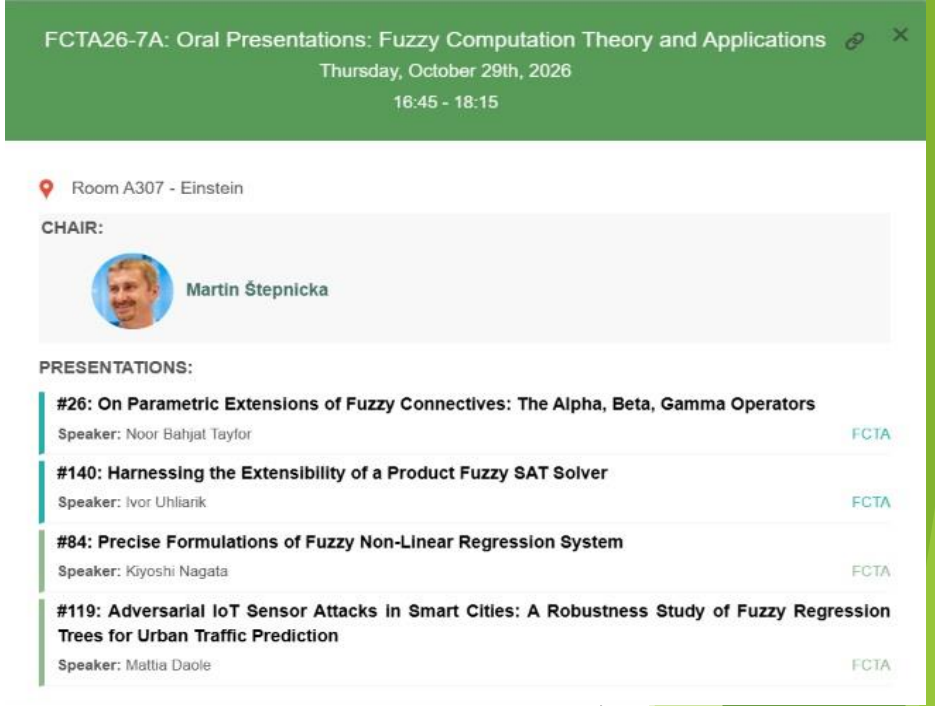
2020年4月～

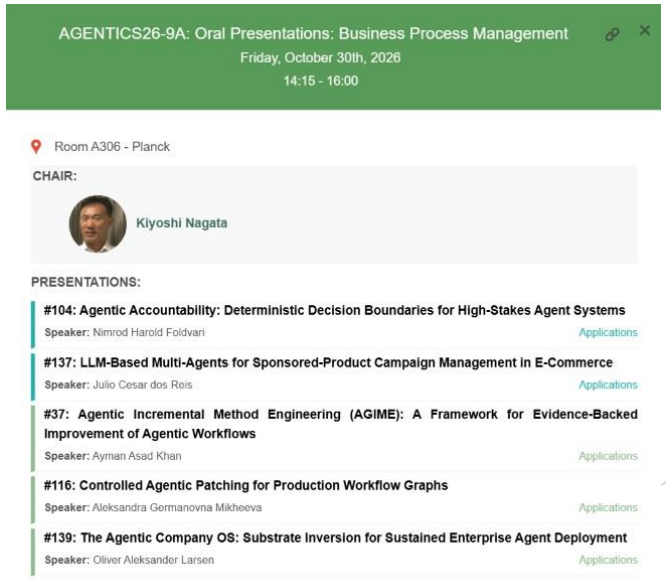
2026年3月

- “Term-based Website Evaluation Applying Word Vectors and Readability Measures”, Proceedings of the 18th International Conference on Web Information Systems and Technologies, 2022/10/25-27, Valletta, Malta
- “Automatic Generating System of Information Security Policy”, *Athens Journal of Technology and Engineering* - Volume 10, Issue 4, 2023/12
- “Establishing Information Security Policy as an Organizational Risk Management”, **In The Future of Risk Management, Chapter 2**. IntechOpen Series, Industrial Engineering and Management, Vol. 9, 2024/1
- “Ontology-based System for Generating Information Security Policy”, Athens Institute Working Paper No. 2025-2787-32, Athens, Greece, 2025/11/14

2026年度と今後の予定

- 2026年9月
  “Developing Java Application for Fuzzy Nonlinear Regression”, Proceedings of the 5th International Conference on ICT Application Research (IAR 2026), 高知
- 2026年10月
  “Precise Formulations of Fuzzy Non-Linear Regression System”, 18th International Conference on Fuzzy Computation Theory and Applications(FCTA26), Angers, France,
  - 発表予定
  - 司会
    - AGECTICS26(2nd International Conference on Agentic and Generative Techniques in Intelligent Computational Systems)- 9A
    - FCTA26-10A

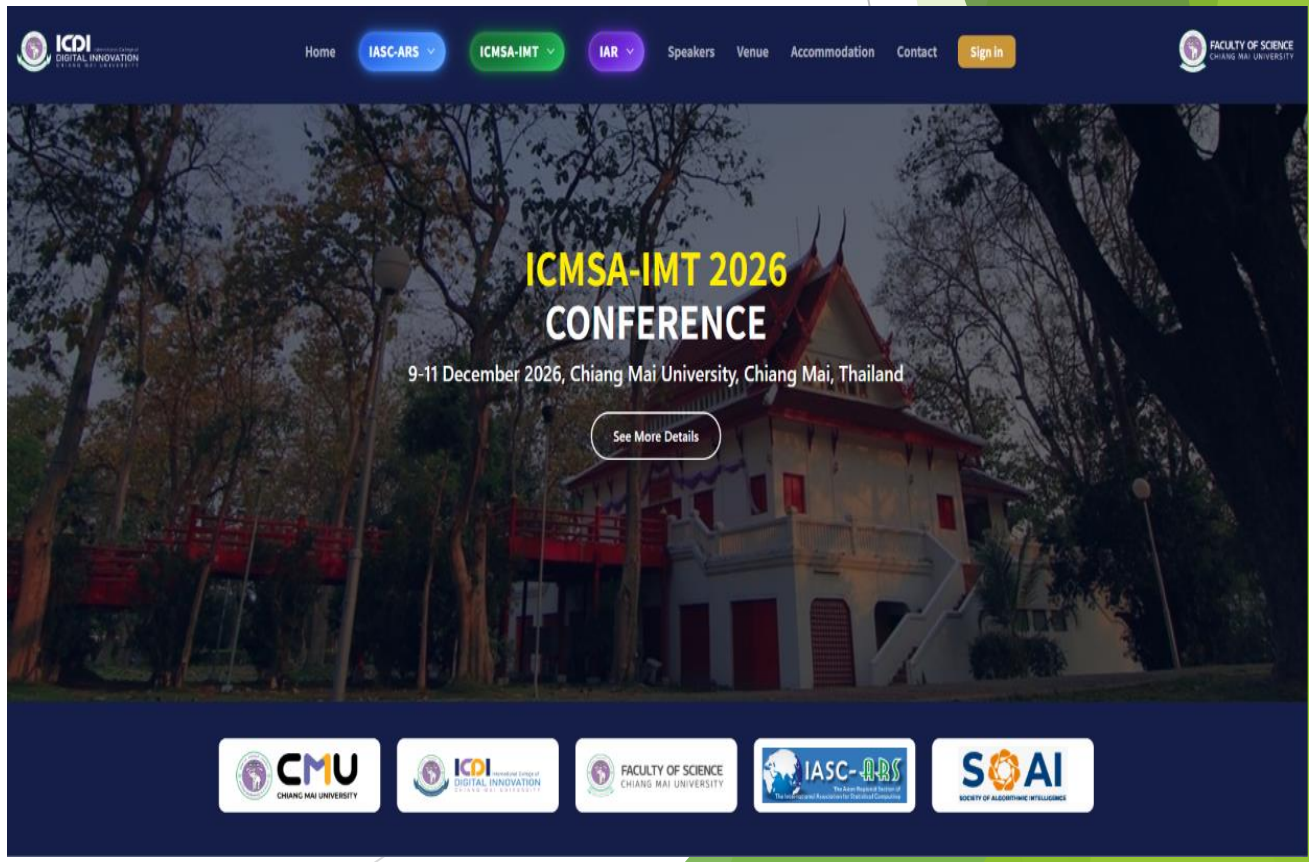






2026年度と今後の予定

- 2026年12月
  The 6th International Conference on ICT Application Research(IAR-6)
  - IAR-6 will be held jointly with the 14th IASC-ARS & SoAI 2026 Joint Conference at Chiang Mai University, Chiang Mai, Thailand,
    from 9 to 10 December 2026
  - 発表予定(???)
  - 司会
  - 運営



今後の予定

- SEAMS School will be held 2027/7/21(Wednesday) 7/30(Friday)



This call is ai
wishing to hos
with CIMPA
opportunity to
and training i
bringing tog
researchers, an
scientific progr
from support
SEAMS–CIMPA
encourage inte
applications be

Cet appel s'
organisateurs
School en parte
offre une excel
recherche et
dans la région
des conféren
étudiants inte
programme sc
écoles sélectio
dans le cadre
Nous encourag
intéressés à so
date limite du 3

