JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

JAIST
21世紀COEプログラム
検証進化可能電子社会

JAIST 21st Century COE Program
Verifiable and Evolvable e-Society

中間報告書

北陸先端科学技術大学院大学　安心電子社会研究センター
Japan Advanced Institute of Science and Technology, Research Center for Trustworthy e-Society

JAIST 21世紀COEプログラム
検証進化可能電子社会 中間報告書

Contents

Message

ご 挨 拶

我々の生活は複雑で大規模な情報システムによって支えられており、その度合いは今後益々加速されることが予想されます。ビジネス効率化のために行われるＩＴ化、政府が推し進めている電子政府計画などのほかに、遠隔教育や遠隔医療など、電子化の波は我々の社会活動のあらゆる側面に及ぼうとしており、我々は本格的な電子社会の時代を迎えようとしています。政治、経済、司法、行政、医療、教育など社会生活の基幹部分のすべてが電子社会システムとして電子化され、これまでにない便利で住み良い社会を作ることが可能になると思われると同時に、情報システムのもつ欠陥や不完全さなどから、不便や不利益を蒙り、さらには、生命や財産の危機に直面することも予想されます。

電子社会のこのような負の側面を解決し、安心して生活を任せられる電子社会を構築するために、情報科学における最新の数理的方法やソフトウェアテクノロジ、人工知能、基盤情報技術などの研究成果を用い、安心な電子社会のための基本概念や技術のための研究教育拠点を確立することが、本COE拠点の目的です。すなわち、電子社会システムを形式的にモデル化し、それが安心であることを形式検証技術やシミュレーションを用いて確認するための方法論、それを安心基盤技術を用いて情報システムとして実現するための研究を行います。それと同時に、教育プログラムの整備により、安心電子社会システムを設計、開発する能力を持った研究者や高級技術者の育成を行います。本拠点計画は、平成16年度に「革新的分野」において採択され、これまでに約2年間活動を行ってきました。本報告では、本拠点の内容やこれまでの活動などについて紹介いたします。

北陸先端科学技術大学院大学
情報科学研究科
21世紀COEプログラム「検証進化可能電子社会」
拠点リーダー　**片 山 卓 也**

拠点形成計画の概要

1．「検証進化可能電子社会」拠点形成計画の目指すもの
－情報科学による安心な電子社会の実現－

今後到来する高度ＩＴ社会では、我々の社会生活は高度で複雑な情報システムである「電子社会」に大きく依存することになる。電子社会とは、我々が営む種々の社会活動のうちで、情報システムによって実現されている部分であり、その役割は、我々の行う社会活動の支援である。電子社会は、我々が社会活動を円滑に行い、安心して生活を送ることができるベースであることから、電子社会の安心性は電子社会に対する最も重要な要求である。最近の情報漏えい問題や情報システムの不具合などは、電子社会の信頼を損ね、社会全体を機能不全に陥れる可能性がある。一方、複雑な年金システムなどのような社会制度自身を，情報技術を使って解りやすく見せることも、安心できる電子社会では実現されなければならない問題である。本 COE プログラムでは、数理的方法やソフトウェアテクノロジ、人工知能、セキュリティやネットワークなどに関する最新の情報科学の成果を利用して、安心な電子社会を実現するための研究教育拠点を確立することを目的としている。

電子社会に安心して生活を任せられるか？

―社会活動の基盤部分を情報システムとして実現
―行政・経済・商業・司法・教育・医療 ...
―社会のインフラ

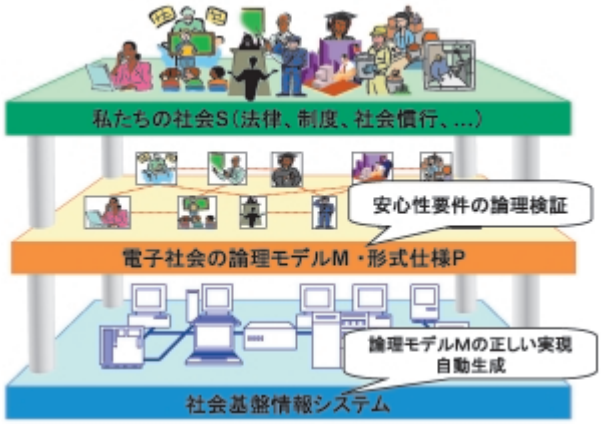
2. 安心な電子社会

電子社会の安心性に我々が期待するものはいろいろであるが、本拠点では、特に基本的なものと思われる以下を主な研究対象とし拠点形成を行う。

- **正当性**
  機能が正しいか？（税額は正しく計算されているか？　処理の内容が法律や制度と整合性があるか？）
- **アカウンタビリティ**
  処理内容や機能についての質問や疑問に対して説明可能か？（なぜ、税額はそのように計算されるか？）
- **セキュリティ**
  プライバシーが守られるか、不正なデータアクセスはないか？
- **進化性**
  社会や環境の変化に適応して、電子社会システムを適切に変更出来るか？
- **耐故障性**
  事故や故障があっても機能し続けるか？
- **高信頼情報基盤**
  高信頼ネットワーク、ハードウェア、ヒューマンインタフェースなどによって実現されているか？

3. 安心電子社会の実現＝形式仕様・モデル化＋形式検証＋安心基盤

安心性の高いシステムの開発には、形式手法が優れている。これは、システムの仕様を形式論理などの数学的な概念を用いて厳密に与え、それにもとづいてシステムの構築を行うものである。この方法論では、情報システムの構築は、（1）仕様の形式化、（2）システムモデルの構築、（3）モデルが仕様を満たすことの検証、（4）安心基盤技術によるモデルの実現、というステップで行われる。仕様は、情報システムの提供する機能やサービスの内容あるいはそれらの満たす性質などを明確に表現したものであり、矛盾を含まず整合性のとれたものでなければならない。また、モデルはシステムの論理的ふるまいを定めたものであり、仕様を満たすことが何らかの方法で検証されなければならない。正しいことが検証されたモデルは、安心性の保障された実装プラットフォーム上に実装され、最終的には計算機システムとして実現される。



4.「検証進化可能電子社会」研究課題と代表的成果

法令文書論理表現と推論、モデル化技術

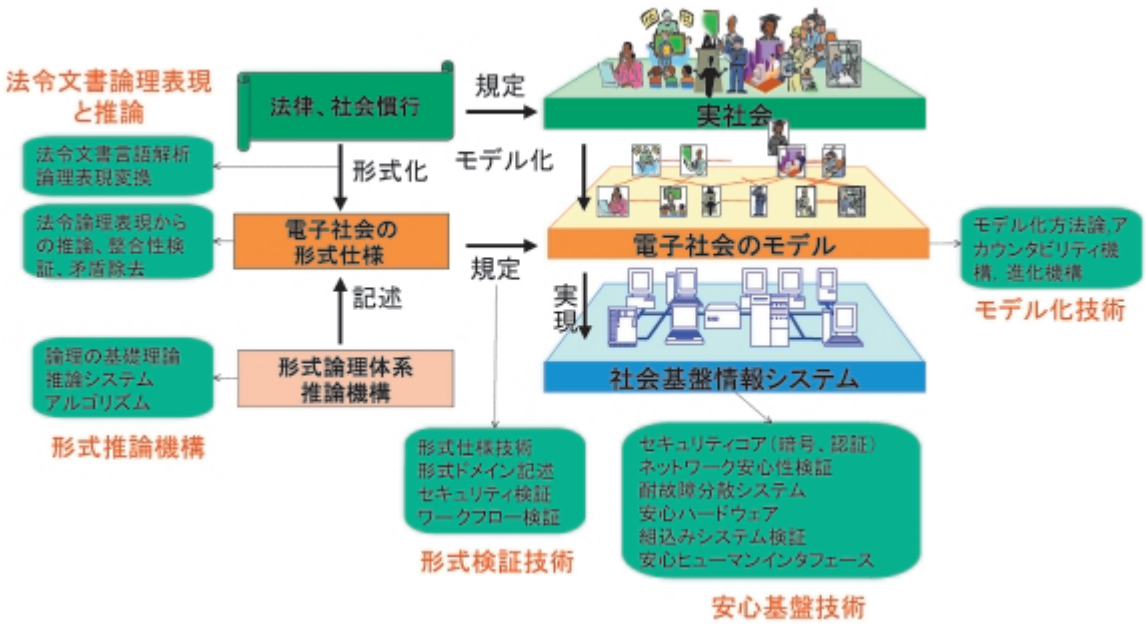
電子社会の仕様は、基本的には、我々の実社会を規定している法律や法令である。このとき、仕様が矛盾を含まず整合的であり、モデルが仕様を満たすことを確実に検証するためには、法令文が形式的に表現されている必要がある。法令文の論理式表現、無矛盾性解析、法令文にもとづく電子社会のモデリング、特にアカウンタビリティと進化機構の研究を行う。

形式検証技術、形式推論機構

電子社会のモデルがその仕様を満たすことの形式検証、形式検証の基礎となる推論機構の研究を行う。
形式検証は定理証明技術やモデル検査などの形式論理学的手法によって電子社会の性質を検証（証明）するものである。より有効な形式検証技術の開発とともに、電子社会を扱うための形式的ドメインモデリングや性能検証などの検証方法論の研究を行う。また、検証の基礎となる推論機構に関しても、その数学的基礎付けやより高度な推論機構の研究を行う。

安心基盤技術

モデルは、最終的にはネットワークやハードウェアから構成される計算機システムによって実現され、また、ヒューマンインタフェース機構が付与されて社会基盤情報システムが構成される。このような観点から、インターネットシミュレータによるネットワーク動作検証、分散システム耐故障プロトコル、高度暗号技術を中心にしたプライバシー保護、暗号専用アーキテクチャ、仕様からの自動合成によるプロセッサの設計、モデル検査による組込みシステムの高信頼化、高度ヒューマンインタフェースの研究を行う。



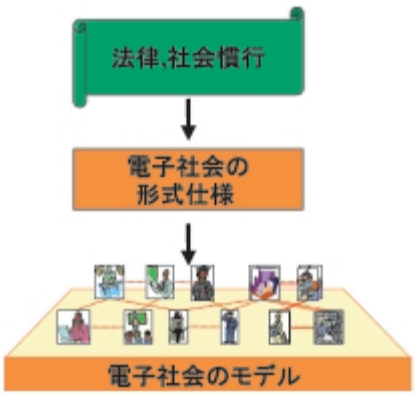
法令文書論理表現と推論、モデル化技術

（島津、東条； 落水、池田、鈴木）

・Law-Defined Information System：「法令文は電子社会情報システムの仕様である」
- 法律の構造にもとづくシステムの構築と進化、アカウンタビリティ機構の導入

・研究内容と成果
- 富山県・千代田区条例の論理式表現、JAIST 規則のアカウンタビリティ機構
- 法令文に適した論理式の決定、法令文 => 論理式変換方式
- 形式推論による法令文論理式データベースからの矛盾の検出・除去アルゴリズム
- 情報システムへのアカウンタビリティ機構組込み方式、法令変更への対応

・法律に基づく情報システム構築の新しい方法論、アカウンタビリティ概念：本 COE の提案



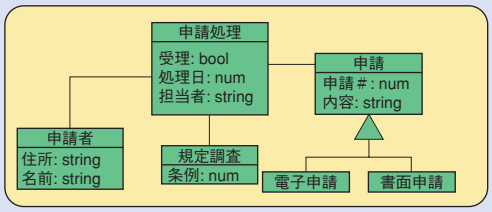
法令文

「県の機関は、申請等のうち当該申請等に関する他の条例等の規定により他の書面等により行うこととしているものについては、当該条例等の規定に関わらず、規則で定めるところにより、電子情報処理組織を使用して行わせることができる。」富山県 54 条 3 項 1 号

アカウンタビリティ：処理内容に関する説明機能

法令変更時の情報システムの変更法

形式推論技術による論理式の矛盾の検出と除去



電子申請行為 (x,y,v,c) ←申請行為 (x,y,a) ∧申請者 (x) ∧県の機関 (y) ∧申請等 (v) ∧書面等 (a) ∧申請手段 (c) ∧規定 (z,v) ∧関連条例等 (z) ∧電子処理組織 (c).

電子社会のモデルと仕様

モデル検査

定理証明

形式検証技術、形式推論機構

（二木、平石、Bjørner、緒方、青木；小野、小川、Vestergaard）

・電子社会の正しさの検証の基幹技術
-電子社会システムの正しさを定理証明、モデル検査、シミュレーションにより検証

・研究内容と成果
-実行可能仕様記述体系CafeOBJとその電子商取引プロトコル安全性
-定理証明システムHOL上のオブジェクト論理とセキュリティ検証
-ワークフローの性能検証・評価システム
-時刻認証アルゴリズムの検証
-形式推論の数学的基礎付け

・形式検証技術に関してわが国最大規模、論理の数学的基礎付けの国際的センター

安心基盤による実現

安心基盤技術

（篠田、Défago、Shen、宮地、双紙、日比野、金子、浅野、赤木、党）

・電子社会モデルを社会基盤情報システムとして実現するための安心技術
-安心ネットワーク技術、セキュリティコア技術、耐故障技術、安心ハードウェア技術

・研究内容と成果
-インターネットシミュレータによるネットワーク検証
-エージェント数理モデルによる安心性検証
-階層的公開鍵暗号方式
-3値論理暗号ハードウェア
-分散システム故障ノード検出方式
-組込みシステムモデル検査方式

・世界最大インターネットシミュレータStarBEDによるネットワーク安心性の実験的検証

研究成果

事業推進担当者

電子社会のための法令文書論理表現と推論

島津 明・東条 敏

電子社会のための形式推論機構

小野 寛晰・小川 瑞史・VESTERGAARD, Rene

電子社会のための形式検証技術

二木 厚吉・平石 邦彦・BJØRNER, Dines・緒方 和博・青木 利晃

電子社会のためのモデル化技術

落水 浩一郎・池田 満・鈴木 正人

電子社会のための安心基盤技術

篠田 陽一・DÉFAGO, Xavier ・SHEN, Hong ・宮地 充子・双紙 正和・日比野 靖・金子 峰雄・浅野 哲夫・赤木 正人・党 建武

ポスドク研究員

松本利雅・NGUYEN, Minh Le・鈴木義崇・大橋功治

情報科学研究科

教授
島津　明
SHIMAZU, Akira
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00039soj.html

研究グループ
電子社会のための法令文書論理表現と推論

専門分野
自然言語処理

拠点形成における研究テーマ
法令文の言語処理

研究の目指すもの

「検証進化可能電子社会」プログラムは、法令は情報システムの仕様であり、その仕様に基づいてシステムの設計や検証をするという新しいパラダイムを提案した。このような考えを具体化するためには、法令文の意味を論理的に表現することが課題の一つとなる。また、システム設計者などの法令理解を支援することが課題となる。本研究はそのような課題を解決することを目指し、法令文を扱う言語処理を研究する。具体的には、法令文の意味を表す論理表現、法令文の意味を表す論理式の記述、法令文から論理表現への変換法、法令文の理解を容易にする支援システムなどを研究する。

拠点形成に関連する最近の研究テーマと成果

（1）法律条文の論理表現形式および論理構造

法律条文の意味をどのような論理形式により表現するか、どのような論理構造により表現するか検討し、法律条文の分析および既研究を踏まえ、第 1 次案を定めた。

論理形式についてはダビドソニアン様式の述語論理表現に様相記号を付加した形式（図 1、3）、論理構造については要件効果構造（田中他，法律条文の標準構造，情処学会，自然言語処理 97-12，1993）の表現とした（図 2）。法律条文には事象を参照する表現があることから、既研究は 1 階述語論理は利用できないとしているが、事象変数の導入により事象参照などを表現することとした。一般に法律条文は社会的な要件のもとで規定される権利・義務を記述している。このような内容は要件効果構造と知られており、この考えに従って、条文の論理構造を表現することとした。

（2） 法律条文の分析と論理式による記述

上記の論理表現形式と論理構造の表現により、具体的対象として、富山県条例第 54 号（全 10 条 34 項）および千代田区条例 53 号（全 28 条 81 項）を取り上げ、それらの条例の項や号の条文の論理表現を記述した（図 3）。法律条文に特徴的な表現、「前項の規定により」、「A、B 等の C」、「A、B その他の C」、「するものとする」などの意味を解釈し、どのように記述するか定めた。

図 1　論理表現の例

「事業者」　区内で事業活動を行う法人その他の団体及び個人をいう。(千代田区53号第2条)

$$\forall x\ \exists e, l\ \text{事業者}(x) \equiv (\text{法人}(x) \vee (\text{団体}(x) \wedge \neg \text{法人}(x)) \vee \text{個人}(x)) \wedge \text{区内}(l) \wedge \text{事業活動}(e) \wedge \text{が}(e, x) \wedge \text{で}(e, l)$$

図 2　要件効果構造の例

公共の場所等において、チラシ等を配布し、又は配布させた者は、そのチラシ等が散乱した場合においては、速やかにこれを回収し、当該公共の場所の清掃を行わなければならない。

（千代田区53号13条2項）

要件部：A【公共の場所等において、チラシ等を配布し、又は配布させた者は】∧
　　B【そのチラシ等が散乱した場合においては】
効果部：A∧C【速やかにこれを回収し、当該公共の場所の清掃を行わなければならない。】

図３　条例の論理表現例

公共の場所等において、チラシ等を配布し、又は配布させた者は、そのチラシ等が散乱した場合においては、速やかにこれを回収し、当該公共の場所の清掃を行わなければならない。

∀x1x2x3x4 ∃e1 e2 e3 e4 e5 人(x1) ∧チラシ等(x2) ∧公共の場所等(x3) ∧人(x4) ∧
((配布する(e1) ∧が(e1, x1) ∧を(e1, x2) ∧で(e1, x3)) ∨(配布させる(e2) ∧
が(e2, x1) ∧を(e2, x2) ∧に(e2, x4) ∧で(e2,x3))) ∧散乱する(e3) ∧が(e3, x2)
⇒O(回収する(e4) ∧が(e4, x1) ∧を(e4, x2) ∧速やかに(e4) ∧
清掃する(e5) ∧が(e5, x1) ∧を(e4, x3))

(3)　法律条文の論理式への変換法

二つの方式を研究した。一つは人手で記述した規則やヒューリスティックスを用いる変換システム、もう一つはコーパスと機械学習に基づく変換システムである。

第１の変換システムは、段階的に条文の言語解析を進め、論理式を組み立てる。段階的な言語解析は、形態素解析、構文解析、要件効果構造の解析、関係表現の解析、格構造および名詞句の解析からなる。

形態素解析と構文解析は条文の係り受け構文木を求める。形態素解析は JUMAN、構文解析は KNP を用いた。要件効果構造の解析は、係り受け構文木から、法律条文に特徴的な表現を用いて要件効果構造を構成する各部を切り出し、各部の論理関係を求める。要件効果構造の各部は、主題、条件、対象、規定である。特徴的表現は上記の富山県と千代田区の条例により求めている。関係表現の解析は、文構成素が原因、目的、対象、状況などの関係になっている場合を求める。格解析は、法律条文の特徴を反映する格フレーム辞書やヒューリスティックスにより動詞と名詞の関係を解析する。格要素の特別な場合は、動詞がフィラーとなる。格フレーム辞書も上記条例に基づく。関係表現の解析、格解析、名詞句解析がそれぞれ原始文を組み立て、それらを要件効果構造の解析で求めた論理式に組み込み、全体の論理式を組み立てる。

要件効果構造の解析を金沢市条例４号（全 28 項）に適用した結果、条件、規定は 100% 解析でき、主題や対象は 33% の見落としがあったが、誤りはなかった。格解析については、不正解は辞書項目がないか、誤構文解析が原因であった。名詞句は簡単な場合しか扱っておらず今後の課題である。

第２の変換システムは、先ず、入力文からその構文意味解析木を求める分類器を機械学習により求め，次に、この分類器を用いて入力文からその構文意味解析木を求めて、その解析木から論理表現を組み立てる。分類器は、構文解析過程の学習に基づくものと、構造 SVM によるものを試みた。構造 SVM を RoboCup におけるロボットの制御用文とその構文意味解析木に適用した実験では、精度 85%、再現率 74% で構文意味解析木が求められた。既研究では、精度 89%、再現率 72% が報告されている。

(4)　法律条文の表示法

法律条文の特徴表現に加え、条文の読点の制約も利用して、要件効果構造の各要素を分割表示する方法、特に、並列句については法律条文の接続詞の使用法の制約も考慮して構造的に表示する方法を試み、テキストと構造表示のどちらがよいか効果をみる実験をした。条文全体の表示については人により違いがあるが、並列句については構造表示の方がよいという結果であった。

拠点形成に関連する主な業績

[1] Minh Le Nguyen, Akira Shimazu, and Hieu Xuan Phan. A Maximum Entropy Model for Transforming Sentences to Logical Form. Shichao Zhang and Ray Jarvis (Eds.). AI2005: Advances in Artificial Intelligence (LNAI 3809), Springer, pp.800-804, 2005.
[2] Minh Le Nguyen, Akira Shimazu, and Hieu Xuan Phan. Structured SVM Semantic Parser Augmented by Semantic Tagging with Conditional Random Field. In the Proceedings of the 19th Pacific Asia Conference on Language, Information and Computation, pp.167-177, 2005.
[3] Minh Le Nguyen and Akira Shimazu. Learning to Map Sentences to Formal Language with Structured SVM Classification: A Case Study for RoboCup Coach Langugage. In the Proceedings of The third international Conference on Computational Intelligence, Robotics and Autonomous Systems, pp.75-95, 2005.
[4] 江尻 暁，北田安希雄，島津 明．法令文の論理式への変換―論理構造について―．言語処理学会第 12 回年次大会，P4-9, 2006.
[5] 北田安希雄，江尻 暁，島津 明．法令文の論理式への変換―原始文について―．言語処理学会第 12 回年次大会，P4-10, 2006.
[6] 山田大介，島津 明．法令文の言語的特徴を利用した可読性向上のための表示．言語処理学会第 12 回年次大会，P2-1, 2006.

教授
東条　敏
TOJO, Satoshi
http://www.jaist.ac.jp/~tojo

研究グループ
電子社会のための法令文書論理表現と推論

専門分野
人工知能

拠点形成における研究テーマ
電子社会のための法推論機構

研究の目指すもの

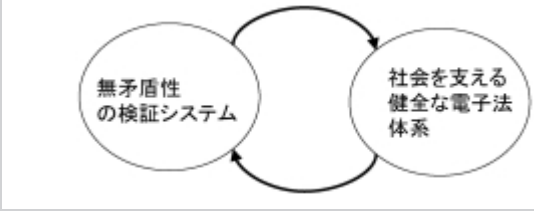
電子化された社会に住む人間の行動を規制するのは法律である。したがって法律文が無矛盾に構成され、その論理的な帰結に齟齬がないことは、安心性の要件の最たるものの一つと考えるべきである。ここで法的推論システムとは、法律文それぞれを、条件部と帰結部からなる「～ならば～」の構造と捉え、それをそのまま論理の推論規則であると考えるシステムのことである。

安心電子社会を規制する法律文による推論とは次の二種類の意味に捉えることができる。

(i) 自然言語で書かれた法律文を論理化・電子化し、われわれを規制する安心な電子法体系を構築する。

(ii) 論理推論システムを法律文の体系そのものに内省させて、そこに齟齬がないか、すなわち無矛盾性の検証システムを構築する。

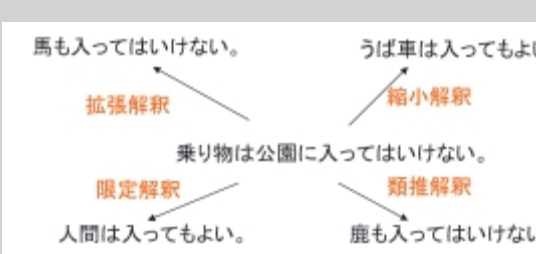
しかしながらこれら二つの概念は相補的なものであり、検証システムは電子化された法体系に働くのと同時に「健全な電子法体系」は常にセルフチェック機能を内在すべきである（右上図）。



法律の推論を困難にしているのはその論理化である。右下図にあるとおり、規制に関する表現は常に解釈の幅を含む。

・「乗り物は入園不可」∀x[乗り物(x)→¬入園可(x)]
・「うば車は入園可である」∀x[うば車(x)→入園可(x)]
・「うば車は乗り物である」∀x[うば車(x)→乗り物(x)]？

またこの例が物語るように法律文は常に例外や但し書きなど後からの補筆改正にさらされ、体系内部での一貫性保持が問題となってきた。従来的な非単調論理や信念修正によって解決できる問題もあるが、これらの手法はあくまで古典論理を基にするため限界がある。本研究の目指すところは新しい論理を法の一貫性保持に応用することである。



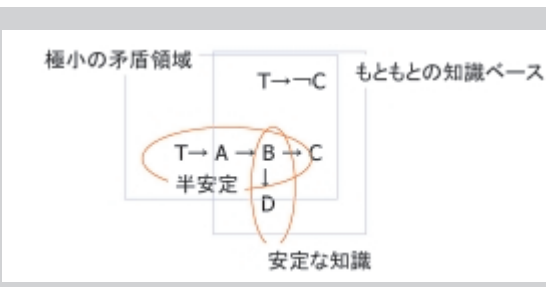
拠点形成に関連する最近の研究テーマと成果

テーマ１：法律知識ベースの矛盾領域の特定

論理における矛盾とは、ある知識ベースにおいてある命題Aとその否定形¬Aが同時に現れることである。したがって人間から見れば明らかに矛盾に見える知識ベース {A→B、A→¬B} はこのままでは矛盾していない。したがって知識ベースを機械的に処理し、この中に矛盾を検出しようとしたら、この知識ベースにファクト（「→」を含まない単体の命題）Aを付加し、Bと¬Bを現出させなければならない。するとここの課題は以下のようなサブテーマを含む。

(i) ある知識ベースのすべての「→」を含む推論式を起動させる最小限のファクトのセットを発見する。
(ii) それにより、知識ベースが矛盾を含むか否か判別する。
(iii) 矛盾に寄与する推論式を特定する。
(iv) これにより、知識ベースの中で極小の矛盾領域を決定する。

右図ではファクトTを追加した結果、すべての推論式が起動され、C と¬C が現れた状態である。この中で B→D はこの矛盾とは無関係である。他の推論式はいずれも矛盾に寄与する可能性がある。また極小の無矛盾領域はこれら半安定な式全体を含む領域となる。



テーマ２：相対的な否定を含む推論

法律の推論を行うに当たっては先のテーマで述べたように論理的矛盾と現実世界での意見対立には大きな隔たりがあることが問題である。この研究では、従来一種類の否定辞（¬）を用いることによる弊害をその動機とする。例えば「正当防衛は合法である」という一文を述語論理に表現するとき、

▶防衛行為は罪にはあたらない。∀ x[行為 (x) ∧防衛 (x) →¬罪 (x)]

▶防衛行為は正当である。∀ x[行為 (x) ∧防衛 (x) →正当 (x)]

という複数種類の書き方が存在しうる。最初の例では「罪」自体に否定的なニュアンスがあり、それをさらに否定辞で打ち消すという書き方になっている。このように自然言語の意味を記号化するに際しては常に恣意性があり、論理化を困難にしている。このテーマでは一般的な否定辞 '¬' を取り除き、二つの命題ϕ、ψに対して互いが対立するという概念のみで論理推論を行うことを目標とする。このとき命題ψが命題ϕに対して相対的に否定されるとし、以下のように書く。

$$\Delta \vdash \neg_{\varphi}\psi \quad \Leftrightarrow \quad \Delta \vdash \varphi \quad \text{かつ} \varphi \wedge \psi \vdash \bot$$

この相対的な否定は、一般的な否定より弱い否定である。以下のように知識ベースΨは¬βを含むが、αに対する相対否定は含まない。

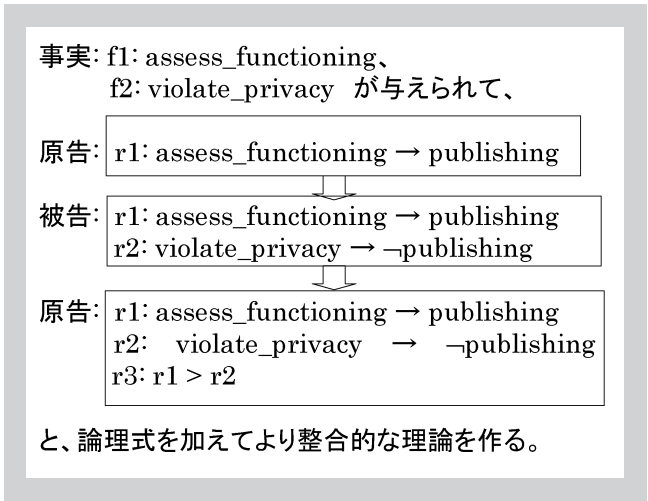
$$\text{If} \quad \Psi = \{\neg\beta, \gamma\}, \ \text{then} \ \ \Psi \not\vdash \neg_{\alpha}\beta.$$

この相対的な否定は、一般的な否定より弱い否定である。以下のように知識ベースΨは¬βを含むが、αに対する相対否定は含まない。また以下のように極小否定の概念を定義することができ、ある命題と対立する命題を極小に特定することができる。

$$\Delta \vdash \ominus_{\alpha}\beta \quad \text{iff} \begin{cases} \Delta \vdash \neg_{\alpha}\beta, \ \textit{and for any} \ \varphi \ \textit{s.t.} \ \Delta \vdash \neg_{\varphi}\beta, \\ \vdash \varphi \rightarrow \alpha \ \textit{implies} \ \vdash \alpha \equiv \varphi. \end{cases}$$

テーマ３：理論に基づく法的論争

本研究においては法廷において原告と被告による論争をモデル化する。法的論争は各プレイヤーが互いに相手よりも優れた理論（法律のルールや解釈を表す論理式の集合）を作ろうとする対話ゲームとして考えられる。ゲームの各プレイヤーは互いに相手の構築した理論に対して何らかの論理式を加えることで、自分の勝利を導き出すような優れた整合性のある理論を構築しようとする（信念強化）。ただし、先のテーマで述べたように法律の理論には矛盾が含まれるので、それを解消するために順序を導入して、より優先度の高い法律を優先する（非単調推論）。例えば右の例で原告が最後に構築した理論にあるようにr1とf1からはpublishingが、r2とf2からはその否定が導かれるが、r3によってr1がr2よりも優先されるので、publishingが導き出される。



拠点形成に関連する主な業績

論文

[1] Y. Suzuki and S. Tojo. Additive Consolidation for Dialogue Games. Tenth International Conference on Artificial Intelligence and Law, 2005.
[2] S. Tojo. Judicial Knowledge Revision with Mimimal Negation. Unilog 2005.
[3] S. Hagiwara and S. Tojo. Stable Legal Knowledge with Regard to Contradictory Arguments, Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, 2006.

著書

[1] 東条 敏．「言語・知識・信念の論理」, オーム社，2006.

教授
小野　寛晰
ONO, Hiroakira
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00035soj.html

研究グループ
電子社会のための形式推論機構

専門分野
形式論理体系の証明論と意味論

拠点形成における研究テーマ
電子社会の記述に使われる論理や形式的体系の数学的基礎づけ

研究の目指すもの

電子社会をモデル化しその安心性要件が仕様をみたしているかどうかを計算機の支援により確認するためには、仕様を形式的に記述し、それを用いて論理的方法により検証することが要である。そのような方法を用いることにより、ソフトウェアの正当性検証において行われているのと同じような形での確実な正当性の保証を得ることが可能になる。

電子社会の仕様は、個人や組織の間の関係、法律上の規定や規制、提供されるサービスや機能などを形式的に記述する必要があるが、さらに社会的な慣行のような暗黙の了解についても仕様として明示的に記述しておかなければならない。本研究の主要な目的は、そのようにして表現された形式的記述を扱うために必要な論理体系について考察し、それらに対する数理論理学的な立場からの基礎研究を展開することである。このような論理体系の選択にあたっては、とくにつぎの二つの点を考慮しなければならない。

▶ 表現力、記述力の豊富さ：時間の推移、行為とプロセス、知識や資源の変化、法的な義務などの様相概念などの記述可能性

▶ 定理証明のアルゴリズムの実効性：非標準論理、一階述語論理（の部分体系）、等式論理のそれぞれが持つ特徴

国際的なレベルの数理論理学の研究を進めるために、海外の研究者との共同研究をおこない、また留学生や研究員を積極的に受け入れている。この 10 数年間に受け入れた海外からの研究者はのべ 100 人を越え、日本の数理論理学研究の中心的な役割を果たしている。

拠点形成に関連する最近の研究テーマと成果

（1）代数化定理

―論理と等式計算における二つの導出可能性の関係

現在進めている「代数的アプローチによる論理研究」についての一連の研究の中で、非標準論理に対する論理体系と代数に対する計算体系である等式計算の間の関係を代数化可能性（algebraizability）の概念を用いて論じた。等式計算は形式的記述の一つの有力な方法である代数的仕様記述の計算として用いられているものである。あたえられた論理が代数化可能であるとは、論理における導出可能性（deducibility）が、対応する代数のクラスが定める等式計算での導出可能性（equational consequence）と本質的に同等になることである。

代数化可能性

その公理がすべて等式で表されるような代数のクラスを等式クラスという。universal algebra での基本的結果により、等式クラスは準同型、部分代数および直積に関して閉じた代数のクラスとして特徴づけられる。
代数化可能性は論理 L の deducibility とそれに対応する等式クラス V における equational consequence を結ぶ一般的なスキーマで、つぎの二つの関係がなりたつことである。

$$s_1, \ldots, s_m \vdash_L t \Leftrightarrow \{s_1=1, \ldots, s_m=1\} \vdash_V t=1$$
$$s_1 \leftrightarrow t_1, \ldots, s_n \leftrightarrow t_n \vdash_L u \leftrightarrow v \Leftrightarrow \{s_1=t_1, \ldots, s_n=t_n\} \vdash_V u=v$$

線形論理や適切含意論理（relevant logic）など、資源を鋭敏に反映する論理（resource sensitive logic）を包括的に議論するための枠組みとして部分構造論理（substructural logic）が知られている。本研究では「すべての部分構造論理が代数化可能である」（代数化定理）ことを明らかにした。この結果により、どんな部分構造論理も等式計算体系として形式化することができることになる。これによりこれらの論理についての性質を議論する代わりにそれを代数の問題に完全に帰着できることになり、したがって universal algebra の方法や結果を有効に利用することが可能になる。

(2) カット除去定理の代数的証明

Gentzen 流のシーケント計算でもっとも基本的な結果はカット除去定理である。このカット除去の持つ代数的な意味を明らかにすることを目標として、その代数的証明を試みた。同時に、これにより代数の研究者に理解し易い形でのカット除去定理の証明をあたえることを目指した。

そのために論理 L のシーケント計算に対応して Gentzen structure を定め、それが L に対応する代数へ準埋め込み可能（quasi-embeddable）であることを示すことにより、カット除去が証明される。この結果からの帰結として MacNeille 完備化とカット除去の関係や、証明探索が有限ステップで失敗したときに有限な反例が生成できることなどの興味深い結果を得た。この代数的な証明法は単に理論的興味にとどまらず、プロセスの表現に用いられる action logic などに応用され今後もさらにこの方向での研究が進展すると予想される。

代数的アプローチによる論理研究

論理を代数的に表現し論理的推論を等式の計算として捉えようという考え方は、その萌芽を 19 世紀のブールやドモルガンの研究に見いだすことができる。ブール代数はもともとそのような考えに基づいて導入されたものであった。20 世紀に入り、タルスキを始めとするポーランド学派を中心に代数的研究は発展し、さらにモデル論との関連の中で universal algebra が誕生した。しかし 1960 年代以降はクリプキ等による可能世界意味論が非標準論理の意味論の主流となった。しかし 10 年ほど前から universal algebra など代数的方法を用いた優れた研究が現れ、代数的方法に対して再評価がおこなわれるとともに関心が高まっている。さらに近年では、これまであまり論じられていなかった証明論的方法と代数的方法の間の密接な関係が明らかにされつつある。

拠点形成に関連する主な業績

主要な論文と研究発表

[1] Francesco Belardinelli, Peter Jipsen and Hiroakira Ono, Algebraic aspects of cut elimination, Studia Logica 77, pp.209-240, (2004).
[2] Hiroakira Ono, Fuzzy logics and substructural logics(招待講演), The 26th Linz Seminar on Fuzzy Set Theory, Linz, Austria (2005).
[3] Hiroakira Ono, Interpolation property and principle of variable separation in substructural logics(招待講演), The 9th Asian Logic Conference, Novosibirsk, Russia (2005).
[4] Hiroakira Ono, Embeddings of algebras and their logical consequences(招待講演), Trends in Logic III International Conference, Warszawa/Ruciane-Nida, Poland (2005).
[5] 小野寛晰 , 論理的方法と代数的方法 (招待講演), 第二回システム検証の科学技術シンポジウム , 大阪 (2005).

特任教授
小川　瑞史
OGAWA, Mizuhito
http://www.jaist.ac.jp/~mizuhito/index.html

研究グループ
電子社会のための形式推論機構

専門分野
理論計算機科学・形式的検証手法

拠点形成における研究テーマ
モデル化と証明に基づく電子社会の安全性検証

研究の目指すもの

電子社会のインフラは巨大化・複雑化がすすみブラックボックスと化している。さらにシステムの正しさは、社会状況により変化するものであり、絶対的な安全性は定義することすら難しい。技術的に可能であり、かつ近年の社会の要請は、いかに納得できるかという安心性と考える。たとえば、セキュリティポリシーに従った実装の保証のレベルを示すITセキュリティ評価・認証制度（ISO/IEC15408）や、会計処理を正しく行われたことを追認可能とすることをめざすSOX法などは、そのような要請の現われである。

本研究ではシステムのモデル化とその性質の証明を通して安心性を与えることを目的とする。モデル化は

（1）数学的モデル　（2）ハイレベルのシステムデザイン・仕様　（3）プログラムコード

の三つのレベルで考えることができる。この中で（2）は、システムの段階的詳細化による設計を想定したシステム設計者の安心性をめざしている。ここではユーザ側の安心性をめざし、（1）と（3）を対象とする。（1）では、証明も納得の手段の一つとしてとらえ、現実の問題をシンプルかつ数学的にモデル化し、その性質を証明する。その際、定理証明系など計算機による証明の自動チェックの支援により、安心性はモデルおよび対象とする性質記述の理解に局所化できる。（3）では、大規模なプログラムコードを想定し、自動抽象化によるモデル生成およびモデル検査によるエラー検出を行う。エラー検出されなくても直接的な保証とはならないが､エラー検出の実績が蓄積されれば、エラー検出されないことは間接的な安心性を与える。

本研究では、上記の設定のもと、アプローチとして（1）に対しては定理証明系Isabelle/HOLの利用による証明の自動チェック、およびモデルのテストデータ実行によるモデル理解支援を行う。（3）に対しては、プログラム解析＝抽象化＋モデル検査というパラダイムに基づき、JavaやMLなどに対する抽象化の設計とその自動化、およびプッシュダウンモデル検査系の利用に基づく自動エラー検出手法の実装を行う。

拠点形成に関連する最近の研究テーマと成果

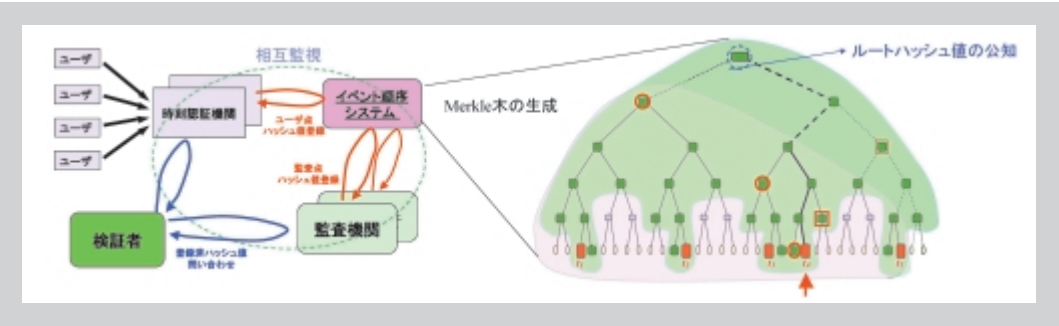
（1）数学的モデルの正当性の形式的証明

A．時刻認証システムの基礎アルゴリズムの正しさの検証（NTTと共同研究）

電子決済や電子オークションなどの普及は、イベントがおきた時刻や順序の認証の必要性を高めている。時刻認証については、大きく分けて、公開鍵暗号に基づくタイムスタンプの電子署名と、ハッシュ関数の一方向性に基づくイベント順序の公知の二つがある。前者は、より時刻精度が高いが暗号の危殆化はすべての認証を無効にする。後者は、公開鍵暗号より頑健と考えられているハッシュ関数にもとづくこと、適当なインターバルでハッシュ値を公開することで、前者の欠点を補完する方式となっている。しかし、いずれの方式においても、認証機関、監査機関などの内部不正に対しては脆弱であった。

NTTの提案するイベント順序証明方式は、後者のハッシュ関数を用いる方式にMerkle木（二分木）を応用することで、単一攻撃点を解消している（すなわち複数の機関が結託しない限り、不正があれば検出される）。さらに実用的な効率を得るために、さまざまなMerkle木上の漸増的アルゴリズムを用いている。

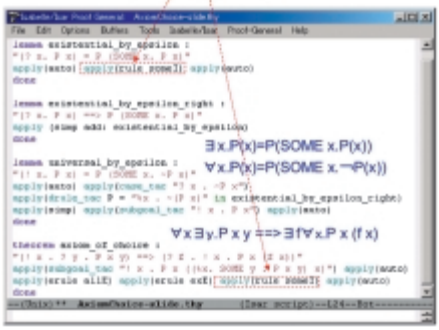
本研究では、Merkle木上の漸増的アルゴリズムのうち、基本的な生成および検査アルゴリズムの正当性を充足可能性検査器MONAを用いて形式的証明を与えた。特に後者の証明はここで初めて与えられた。



B．定理証明系 Isabelle/HOL を用いた Kruskal 型定理の形式的証明・ライブラリ化

近年の定理証明系は成熟を示しつつあるが、いまだライブラリの充実は十分ではない。本研究では、古典的な推論のうち、選択公理（古典的には Zorn の補題と等価）に焦点をあて、Kruskal 型の定理を実際の例として定理証明系 Isabelle/HOL による形式的証明を与える。Kruskal 型の定理は、基礎集合上の順序関係をさまざまなデータ構造上の埋め込みとして自然に拡張する手段を与える。ここでは第一のステップとして、もっとも簡単な有限語上の Higman の補題の形式的証明を試みた。Higman の補題は、Zorn の補題に基づき極小 bad 系列の存在を用いるのが標準的な証明であるが、証明の計算的意味と関連が深い Open 帰納法（通常の WFO 帰納法の拡張）を用いた証明をとりあげ、Open 帰納法のライブラリを構成した。

$$\frac{P\ ?x}{P\ (\mathrm{SOME}\ x.\ P\ x)}\ \mathrm{someI}$$



Hilbert の ε と選択公理

Higman の補題のさまざまな証明

* Higman の補題 (1952 Higman)
* 極小 bad 系列による証明 (1963 Nash-Williams)
* 順序数を用いた構成的証明 (Simposon 1988)
* 正規表現（の変形）を用いた構成的証明 (Murthy-Russel, 1990)
* A- 変換を用いた構成的証明 (定理証明系 *Nuprl*, Murthy 1990)
* Open induction (Coquand 1993, Gaser 1996)
* ….

Open Indution (Raoult 1988)

If $>$ is *downward complete* and P is *open*,

$(\forall x\,(\forall y\,(y<x \Rightarrow P\,y) \Rightarrow P\,x)) \Rightarrow (\forall x.\,P\,x)$

(2) プログラムコードの自動抽象化によるモデル生成とモデル検査

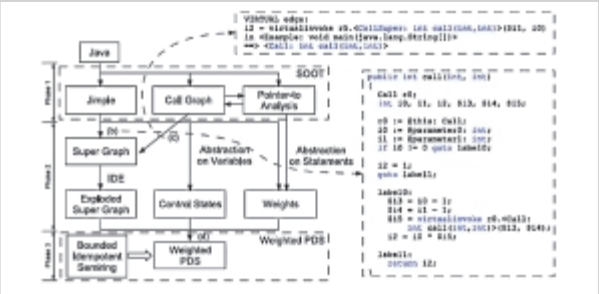
A. 重み付プッシュダウンモデル検査ライブラリを用いた Java プログラムの関数間解析の実装

「プログラム解析の実装＝中間言語＋抽象化＋モデル検査系」という発想に基づき、Java の中間言語 Jimple への変換系として SOOT、バックエンド解析エンジンとして T.Reps のグループが開発した重み付きプッシュダウンモデル検査ライブラリ WPDS を利用する Java の関数間解析の実装法を提案した。状態遷移系へのプログラムの抽象化（モデル化）ができれば、モデル検査系を解析エンジンとして使えることは、90 年代より知られていた。しかし、現実のプログラミング言語は巨大であり、すべての言語要素に対し抽象化を与えるのは容易ではない。本研究では、適切な中間言語とそこへの変換系をあわせて用いることで、非常に簡単な実装が可能になることを示した。今後は、SML# コンパイラ・プロジェクト（東北大学・大堀研）などと連携し、ML のプログラム解析で本手法の有効性を実験する予定である。

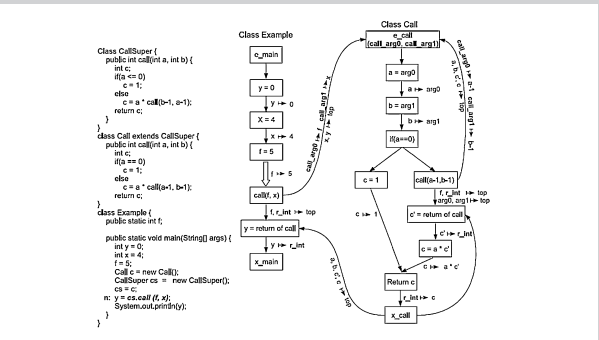
B. 効率的プッシュダウンモデル検査アルゴリズム

汎用解析エンジンとなるプッシュダウンモデル検査は強力ではあるが、現在のところ、巨大プログラムを扱える効率は得られていない。既に提案しているコントロールグラフの代数的構成法を用いた解析アルゴリズムの効率化（M.Ogawa,Z.Hu, I.Sasano, Iterative-free Program Analysis, ACMICFP 2003)を応用し、実用的な効率のアルゴリズムの設計をめざす。

SOOT と WPDS を用いた解析系の構成



Java プログラムのモデルの生成例



拠点形成に関連する主な業績

論文

[1] Mizuhito Ogawa, Eiichi Horita, Satoshi Ono, *Proving Properties of Incremental Merkle Trees*, Proc. 20th International Conference on Automated Deduction, CADE-20, Springer LNAI 3632, pp.424-440 (2005)

[2] Xin Li, Mizuhito Ogawa, *Interprocedural Program Analysis for Java based on Weighted Pushdown Model Checking*, 5th International Workshop on Automated Verification of Infinite-State Systems, AVIS'06, *to appear* (2006)

[3] Isao Sasano, Mizuhito Ogawa, Zhenjiang Hu, *Maximum Marking Problems with Accumulative Weight Functions*, Proc. International Colloquium on Theoretical Aspects of Computing, ICTAC05, Springer LNCS3722, pp.562-578. ICTAC05 (2005)

情報科学研究科

助教授
VESTERGAARD, Rene

http://www.jaist.ac.jp/~kkgi/thisyear/soj/00297soj.html

研究グループ
電子社会のための形式推論機構

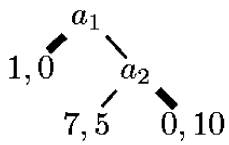
専門分野
Formal reasoning about information structures

拠点形成における研究テーマ
Formal game theory

研究の目指すもの

This research project concerns technical and formalist applications of a recently-developed discrete notion of game-theoretic Nash equilibrium [1]. It focuses on the benefits of knowing why something is an equilibrium in a variety of applications and on understanding in more detail the different kinds of (game-theoretic) compromises between the agents that are prescribed by the traditional probabilistic approach and our novel rewriting-based approach to game theory.

Game theory aims to study situations with conflicts of interest in a very general sense. In particular, non-cooperative game theory, due to Nash, aims to predict what will happen when autonomous agents that either have no means or no interest in interacting are accessing the same resource. One way of accessing a resource is sequentially: agents make a sequence of choices that results in some outcome. An example is as follows.



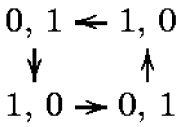
Two agents, a1 and a2, participate in the example: a1 chooses first and a2 may be called upon to choose second. The leafs indicate the payoffs to the agents when the game ends there: a1's first and a2's second. In this kind of games, called extensive form, Nash equilibria consist of a complete set of choices in all internal nodes, irrespective of whether the node is reached. The set of choices indicated by thick lines in the example is the only Nash equilibrium: a2 is happy (in Nash's technical sense) because his choice does not affect the considered outcome and a1 is happy because his other choice gives him a lower payoff. The outcome giving 7 to a1 and 5 to a2 is not involved in a Nash equilibrium because either a1 or a2 could improve their outcome by changing their choice, depending on a1's choice. Compromises are not needed for extensive-form games [2]. The same is not true for simultaneous games; an example, using strategic form, is as follows, with two agents playing: vertical chooses the row and gets the first payoff, horizontal chooses the column and gets the second payoff. In no cell are both agents happy.

	h_1	h_2
v_1	$0, 1$	$1, 0$
v_2	$1, 0$	$0, 1$

Game theory is traditionally applied in social sciences and particularly in economics. As a result, game theory, as currently considered, defaults to using probabilities for expressing any and all notions of compromise between agents. In the example, the only probabilistic Nash equilibrium consists of both agents choosing between their two options with equal probability, with an expected payoff of 1/2 to each.

By contrast, and in order to address formalist and technical application areas, we have developed a discrete notion of Nash equilibria that we have proved exist for a very large class of games (that subsumes Nash's notion of strategic-form games) [1]. This new notion of Nash equilibria, which we call change-of-mind equilibria, have a range of meta-theoretic properties that probabilistic Nash equilibria do not; the most important of these is the fact that change-of-mind equilibria are directly characterised, i.e., they come with an inherent topology that shows exactly why this particular compromise is considered to be an equilibrium

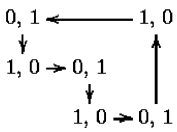
[1]. In the strategic-form example above, the change-of-mind equilibrium is the cycle indicated below.



A change-of-mind step indicates that the agent in question, horizontal/vertical, can and wants to move away.

It is worth noting in the example above that both the probabilistic and the change-of-mind approach involve all four cells in their prescribed equilibrium. A generalised version of the example is as follows, on the left.

	h_1	h_2	h_3
v_1	0, 1	0, 0	1, 0
v_2	1, 0	0, 1	0, 0
v_3	0, 0	1, 0	0, 1



The only change-of-mind equilibrium is shown on the right. As before, the only probabilistic Nash equilibrium consists of both agents assigning equal probabilities to their three options, with expected payoffs of 1/3.

A slightly differently flavoured version of this example is as follows.

	h_1	h_2	h_3
v_1	0, 1	−7, 0	1, 0
v_2	1, 0	0, 1	−7, 0
v_3	−7, 0	1, 0	0, 1
v_4	0, 0	0, 0	0, 0

The change-of-mind equilibrium is the same cycle just considered. Any probabilistic Nash equilibrium, however, have vertical putting full weight on his last option, the lower row.

What the examples show is that the two notions of equilibria involve different parts of the considered games, in many different configurations. That said, it is also the case that a singleton instance of either notion of equilibrium is a singleton instance of the other notion and more work is required before either notion is properly understood.

拠点形成に関連する最近の研究テーマと成果

The COE part of the project concerns applications of rewriting game theory and focuses diarectly on e-society issues, such as digital rights/licensing [3] and networking [4,5], and, more generally, on informatics treatments of core economics, e.g.,

- Aumann's Theorem on Rationality concerning the benefits of sustained involvement in conflict resolution [6],
- Coase's Principle concerning public legislation vs private negotiation for resource-access rights, specifically for resources that are evolving and usage patterns that are speculative about the evolution of the resource [7],
- Kahneman and Tversky's Prospect Theory concerning subjective assessments of gain and loss [8].

Other parts of the project aim to address issues, e.g., in Systems Biology [9,10].

拠点形成に関連する主な業績

[1] "Rewriting Game Theory and Nash's Construction", Le Roux, Lescanne, Vestergaard.
[2] "A Constructive Approach to Sequential Nash equilibria", Vestergaard.
[3] "Digital Rights: Consumers and Producers in a Digital World", Futatsugi, Bjorner, Vestergaard, Ogata, et al.
[4] "A Rewriting Game Theory Analysis of a Dynamic Router Layer", Kokai, MSc thesis (Vestergaard).
[5] "A Rewriting Game Theory Analysis of IPv6", Kumamoto, MSc project (Vestergaard).
[6] "The Inductive and Modal Proof Theory of Aumann's Theorem on Rationality", Vestergaard, Lescanne, Ono.
[7] "A Game Theoretic Approach to Coase's Principle with Evolving Harm", Tanaka, MSc thesis (Vestergaard).
[8] "A Rewriting Game Theory Analysis of Prospect Theory", Tachibana, MSc project (Vestergaard).
[9] "A Discrete Game-Theoretic Foundation for Signal Transduction", Vestergaard, Senachak, Vestergaard.
[10] "A Discrete Game-Theoretic Foundation for Gene Regulation", Vestergaard, Delaplace, Lescanne, et al.

情報科学研究科

教授
二木　厚吉
FUTATSUGI, Kokichi
http://www.jaist.ac.jp/~kokichi

研究グループ
電子社会のための形式検証技術

専門分野
形式手法とソフトウェア工学

拠点形成における研究テーマ
ドメインモデルの形式記述と検証

研究の目指すもの

検証進化可能な電子社会を構築するための基盤技術として、電子社会において基本的なドメインモデル（domain model）の形式記述（formal description）を作成しそれを解析・検証する技術を研究開発する。ドメインは同一の特徴を共有するシステムの集合であり、検証進化可能な電子社会の実現のためには、ドメインのモデルを作成しその性質を解析する技術が重要となる。

Domain Engineering and Digital Rights Group (http://www.ldl.jaist.ac.jp/drcp/) として研究チームを組織し、以下のテーマについて研究を進める。

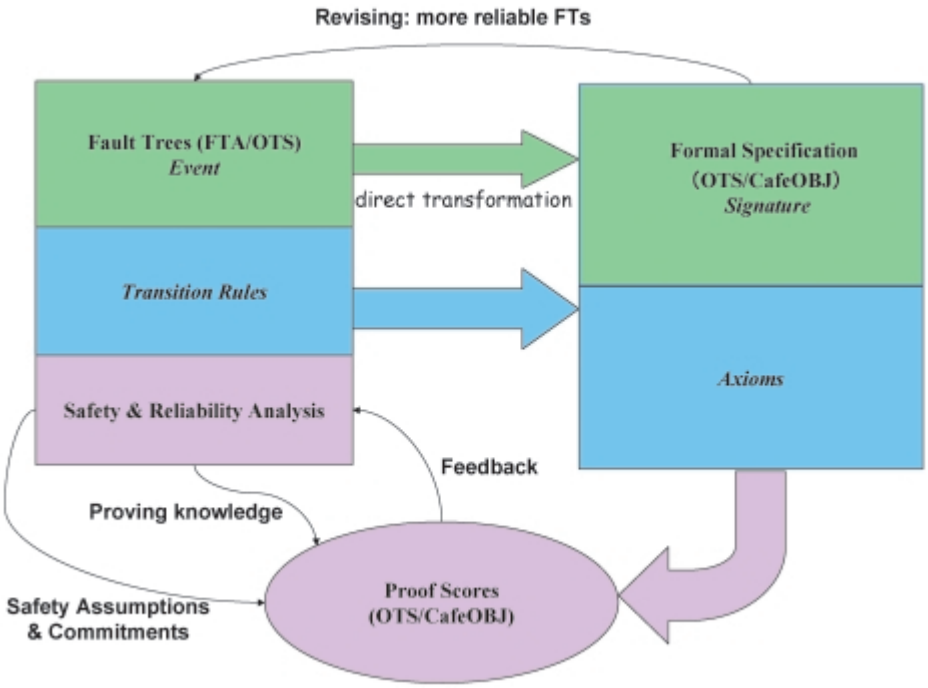
(1) ドメインモデルの形式記述の作成法：Digital Rights（電子ネットワーク社会における音楽や映像を含む広義のドキュメントの権利）のドメインに焦点をあて実行可能形式仕様言語 CafeOBJ による形式仕様の作成を通じて、形式記述の作成法を研究開発する。

(2) ドメインモデルの解析・検証法：CafeOBJ 言語システムを用いたシミュレーションや証明スコア法による検証を発展させ、Digital Rights ドメインにおいて有効な解析・検証法を研究開発する。

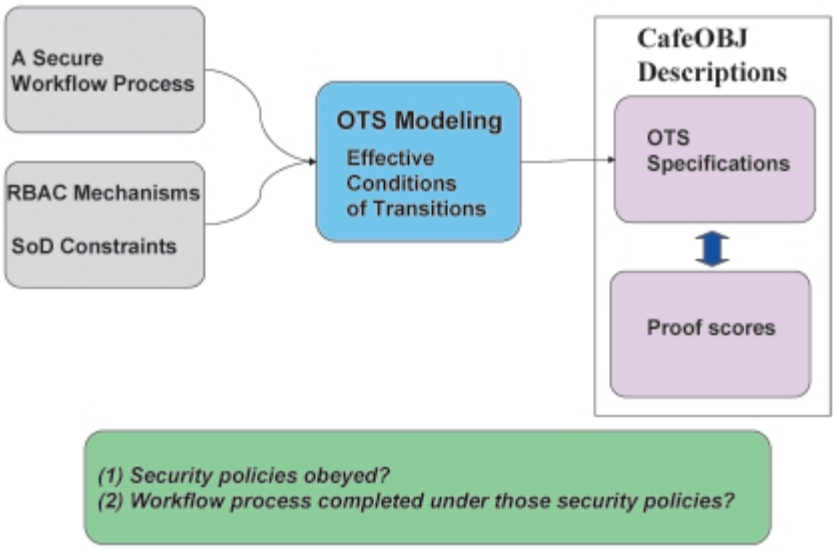
拠点形成に関連する最近の研究テーマと成果

10 年以上にわたる国際的な研究開発活動の成果である実行可能形式仕様言語 CafeOBJ を中核として形式手法（formal methods）の研究を展開している。2004 年度、2005 年度における研究テーマと成果は以下のようなものである。

失敗木解析（fault tree analysis）の形式化とその要求工学への適用：
失敗木解析は開発すべきシステムへの要求を記述・解析する手法として、長い歴史を持ち、開発現場での実績も豊富である。その適用範囲を広げ、より厳密な解析を可能にするために、CafeOBJ に基づく OTS（Observational Transition System）モデル（OTS/CafeOBJ）により失敗木解析を厳密に形式化し、それを用いた要求解析の方法を開発した。



セキュリティを考慮したワークフローモデルの定式化と解析：ワークフローモデルはビジネスにおける業務分析等に広く用いられ、既に商用のサポートツール等も開発されており、セキュリティを考慮したモデルの開発は安全性への要求が高まるにつれて重要性を増している。本研究では、セキュリティを考慮したワークフローモデルを OTS/CafeOBJ を用いて定式化しその検証法を開発した。



形式仕様における適切な抽象度の研究：

形式仕様にいかにして適切な抽象度を持たせるかは、形式仕様の実用性を高める上できわめて重要である。本研究では、今まで開発した CafeOBJ の形式仕様の事例を解析することで、（1）データ型とプロセス型を適切に使い分けることで適切な抽象度のモデル化が得やすく、（2）データ型は比較的汎用的に利用でき、プロセス型は問題領域に依存する可能性が高い、といった知見を得た。これらの結果は、より整理・体系化することで、さらに実用的な方法論に発展し得るものである。

探索型と推論型を融合した検証法の研究：

モデル検査器に代表される探索型の検証と定理証明期に代表される推論型の検証を融合することはシステム検証における重要なテーマである。本研究では、CafeOBJ の証明スコア法による対話型検証において、探索型のモデル検査器を用いた自動検証・反例発見と対話型の推論型の検証を使い分けることが有効であるとの知見を得た。これに基づき、CafeOBJ と同系の代数仕様言語である Maude 言語のモデル検査器への CafeOBJ からの変換法を開発した。

拠点形成に関連する主な業績

[1] Kokichi Futatsugi, Joseph Goguen, and Kazuhiro Ogata: Verifying Design with Proof Scores, Proc. of 1st IFIP-WG2.3 Conf. on Verified Software: Tool, Theory, and Experience (electric form), October 2005.

[2] Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi: Formal Analysis of Workflow Systems with Security Considerations, Proc. of the 17th International Conf. on Software Eng. and Knowledge Eng., pp.531-536, September 2005.

[3] Kazuhiro Ogata and Kokichi Futatsugi: Equational Approach to Formal Analysis of TLS, Proc. of the 25th Intl. Conf. on Distributed Computing Systems, IEEE Computer Society Press, pp.795-804, 2005.

[4] Takahiro Seino, Kazuhiro Ogata, and Kokichi Futatsugi: Mechanically Supporting Case Analysis for Verification of Distributed Systems, Journal of Pervasive Computing and Communications, 1(2): 135-145, Troubador, 2005.

[5] Jianwen Xiang, Kazuhiro Ogata, and Kokichi Futatsugi: Formal Fault Tree Analysis of State Transition Systems, Proceedings of the 5th Intl. Conf. on Quality Software, IEEE Computer Society Press, pp.124-131, 2005.

情報科学研究科

教授
平石　邦彦
HIRAISHI, Kunihiko
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00057soj.html

研究グループ
電子社会のための形式検証技術

専門分野
システムの形式的モデル化と検証・最適化

拠点形成における研究テーマ
ビジネスプロセスの安心性検証

研究の目指すもの

電子社会では、行政・企業の様々な業務が情報システムの統合により遂行される。米国における SOX 法に見られるように、組織内の各データや業務プロセスを明確化し、透明性を確保することが社会的に求められている。このような要求に対し、組織内あるいは組織間の業務の流れを定義したワークフローによるビジネスプロセスの管理は有効な手段とされている。本研究は、計算機科学の手法を用い、電子社会におけるビジネスプロセスの安心性を以下の２つの側面から検証する方法を開発することを目標とする。

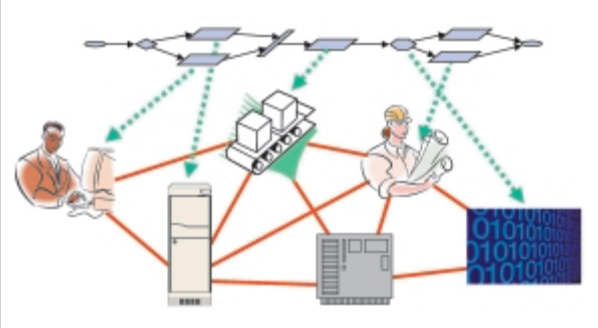
▶論理的な安心性：組織に関するドメインモデル（組織構造、役割、権限、責務、承認／報告フロー、業務規則など）とワークフローの整合性検証。実行時のモニタリング手法。

▶性能面での安心性：ワークフローが必要な処理能力を持つかどうかの検証。最適な資源配分の決定方法。

ワークフロー（Workflow）とは

ビジネスプロセスの全体またはその一部を自動化するものであり、これにより、ドキュメント・情報・タスクが、手続き規則に従って、担当者から担当者へ受け渡されていく。（WfMC：http://www. wfmc.org/ の定義）。
最近では、情報システム構築における設計と実装とを繋ぐ手段、あるいは、複数の情報システムを統合する手段としてビジネスプロセスのモデル化が重要視されている。

図１．電子社会におけるワークフローの概念：
ワークフローは人、システム、情報を統合する。



拠点形成に関連する最近の研究テーマと成果

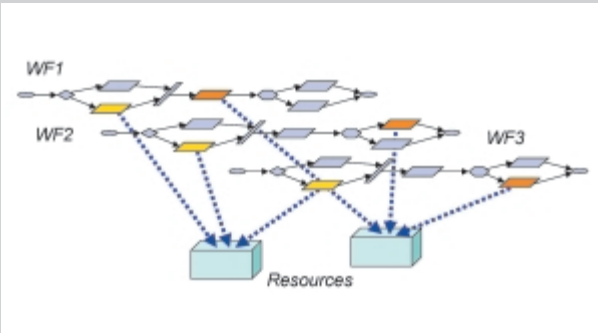
（1）確率モデルを用いた並行ワークフローの性能評価と最適な資源配分の決定

ワークフローはたとえ論理的に正しく設計されていても、同型の多数のフローが並行に処理されることにより、性能低下やシステムダウンなどを引き起こす可能性がある。ワークフローシステムの性能面での安全性を検証するための方法として、確率モデルを用い、システムの安定動作に必要な資源量を評価する手法を提案し、その有効性を確認した。

適用事例

学術論文誌の査読プロセスは個々の論文に対する多数の査読フローが並行して流れるワークフローとしてモデル化できる。また、ランダムにジョブを投入してくる論文投稿者に対して、継続的にサービスを提供するビジネスプロセスでもある。これを例題とし、ワークフローを確率ペトリネットでモデル化することにより、適切な編集委員数を算出した [1]。

図２．並行ワークフローにおける資源配分問題
（各資源は同時に複数のフローに関係する）



(2) ハイブリッドシステムの設計・検証問題に対する記号計算アプローチ

連続・離散変数上の複雑な制約条件を扱うことのできるダイナミカルシステムであるハイブリッドシステムに着目し、制約充足に基づく記号計算アルゴリズムを用いた効率的な計算方法について研究を行った [2,3]。ハイブリッドシステム表現をワークフローの解析に用いることにより以下が可能になる。

▶時間制約や資源制約を含むワークフローの動作検証をハイブリッドシステムの検証問題として一般的に取り扱うことができる。

▶作業時間や必要な資源の見積もりなど不確実なデータを含む場合、それらを数値ではなく数式の制約条件により規定される領域として扱うことができる。

▶多数のフローを連続量として抽象化して扱うことができる。

今までの成果

1. ハイブリッドシステムにおける基本的計算（制約充足、凸多面体操作、線形および 2 次形式最適化）および探索における分枝限定操作をサポートする制約論理プログラミング言語 KCLP-HS の開発（図 4）。
2. 記号計算アルゴリズムである QE（Quantifier Elimination、一階述語論理式から限量子 ∀、∃ を取り除いた等価な論理式を求める手法）を用いた検証手法に関する研究。
3. 混合論理ダイナミカルシステム表現を用いたハイブリッドシステムの最適化手法の高速化に関する研究。

ハイブリッドシステム（Hybrid Systems）とは

オートマトンにより記述されるデジタル動作（離散事象系）と微分方程式により記述されるアナログ動作（連続系）が混在するシステムであり、自動車や航空機、プラント制御などの組込み制御システムなど、実世界と計算機が接する様々な場面に出現する。時間制約をもつような実時間システムもハイブリッドシステムの枠組みで扱うことができる。

図 3．連続ペトリネットで表現した査読プロセスのワークフロー（処理能力を上限、下限のインターバルの形で与え、また、ジョブ数を連続量として抽象化している。）

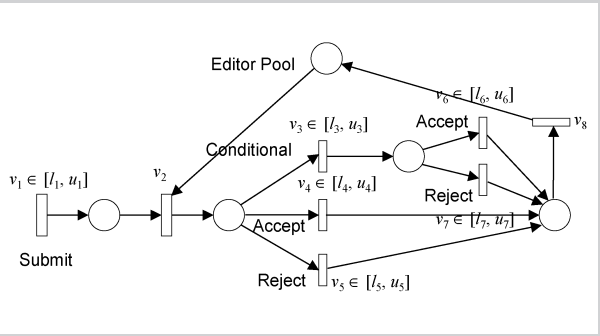
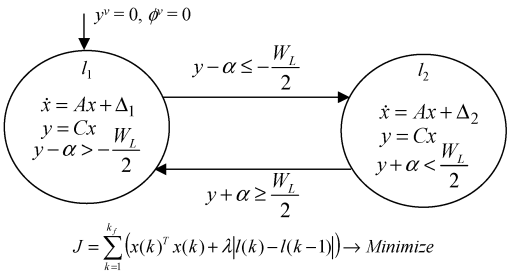


図 4．ハイブリッドオートマトンの動作を記号的にシミュレートするプログラム



ハイブリッドオートマトン

```
go(F, L, A, Z, J):-FinalTime(: F), Lambda(: L), Alpha(: A),
                   min(J, I1(0, 0, 0, 0, J)),
                   project([A], Z).
```

検証・最適化の Query

```
I1(X1, X2, T, J, J):- FinalTime(: FT), T >= FT, !.
I1(X1, X2, T, J, J1):- (optval, !, J <= @optval; true),
        Alpha(: Alpha), X1 + 0.215 * X2 - Alpha > - 0.05,
        I1(X1 + 0.022765 * X2 + 0.000781, X2 - 0.06864,
           T + 0.1, J + X1 * X1 + X2 * X2, J1).
I1(X1, X2, T, J, J1):- (optval, !, J <= @optval; true),
        Alpha(: Alpha), X1 + 0.215 * X2 - Alpha <= - 0.05,
        Lambda(: L), I2(X1, X2, T, J + L, J1).
I2(X1, X2, T, J, J):- FinalTime(: FT), T >= FT, !.
I2(X1, X2, T, J, J1):- (optval, !, J <= @optval; true),
        Alpha(: Alpha), X1 + 0.215 * X2 + Alpha < 0.05,
        I2(X1 + 0.022765 * X2 - 0.00061, X2 + 0.053464,
           T + 0.1, J + X1 * X1 + X2 * X2, J1).
I2(X1, X2, T, J, J1):- (optval, !, J <= @optval; true),
        Alpha(: Alpha), X1 + 0.215 * X2 + Alpha >= 0.05,
        Lambda(: L), I1(X1, X2, T, J + L, J1).
```

KCLP-HS の実行コード

拠点形成に関連する主な業績

主要論文

[1] 小谷正行，平石邦彦，確率ペトリネットを用いたワークフローの性能評価，計測自動制御学会システム・情報部門学術講演会2005，pp.354-359 (2005)

[2] Kunihiko Hiraishi, Sunseong Choe, Computational Tools for Designing Hybrid Systems Based on Constraint Satisfaction, Proc. Workshop on Control of Hybrid and Discrete Event Systems, Satellite workshop of ATPN2005, pp.41-60 (2005)

[3] Sunseong Choe, Kunihiko Hiraishi, Application of Quantifier Elimination to Optimal Control Problems of Hybrid Systems, Proc. 7th Asian Symposium on Computer Mathematics, pp.62-65 (2005)

情報科学研究科

特任教授

BJØRNER, Dines

http://www.jaist.ac.jp/~bjorner

研究グループ
電子社会のための形式検証技術

専門分野
Software Engineering and Programming Methodology

拠点形成における研究テーマ
Formal Description and Verification of Domains

研究の目指すもの

Domain Engineering and Digital Rights & Obligations

During my one year stay at JAIST COE I shall research and lecture about two related areas:

- Domain Engineering
- Digital Rights & Obligations: Consumers and Producers in a Digital World

拠点形成に関連する最近の研究テーマと成果

Domain Engineering

What is a Domain?

- Examples of societal infrastructure domain components are:
  - financial services (actions within and between clients, banks, insurance companies, stock and bond brokers and exchanges, etc.),
  - health care (actions within and between patients, private physicians, pharmacies, hospitals and clinics, the pharmaceutical industry, etc.),
  - transportation (actions within and between user of and the road, railway, etc., systems themselves)
- Document handling in all its generalities is also a domain (document operations: creation, editing, viewing (rendering), copying, distribution, and shredding, etc.; document categories: templates, forms, aggregates, etc.; document attributes: rights and obligations with respect to categories and operations—security, access, availability, etc.).

What is Domain Engineering?

- It is the research & advanced engineering,
- i.e., the experimental development of
- comprehensive informal and formal descriptions of domains
- and their formal analysis.

How to Pursue Research in Domain Engineering?

- Through interaction with domain stakeholders (owners, managers, workers, clients)
  - to create precise ontologies, informal and formal,
  - to create precise descriptions, informal and formal,
  - to build theories about these domain, that is: analysis and proofs of properties.
- Through experiments like the above
  - to further develop and research domain engineering methods: principles, techniques and tools,
  - to study ontologies emerging from the specific domain theories, and
  - to possibly establish a theory of infrastructures—trying to answer the question: "*What is an Infrastructure?*".

Digital Rights & Obligations

Patents Versus Licenses

Todays conventional world of digital rights appears to be conceived in a context void of understanding the relations between

- the concepts of intellectual property rights, copyrights, patents, trademarks, etc.,
- the ownership of such protected works (as purchased)
- and the enforcement of their infringement by laws (implying financial and other forms of punishment) etc., on one hand, and
- the concepts of licensed works to be operated upon by consumer-owned devices and possibly edited, rendered, copied, and distributed,
- and the enforcement of their infringement (implying injunctions).

The current thoughts, plans and implementation of so-called digital rights management appears not to consider the implications of a clearer understanding of the above relationships.

What is "Digital Rights"?

- Digital rights secure that owners of intellectual works (literature, music, movies, etc.)
- are paid by such consumers who render (read, play, view, etc.) the works and
- according to license agreements between owners and consumers.

What is "Digital Obligations"?

- Digital Obligations secure that users of intellectual works
- have fair access to and handling (copying, editing, viewing (rendering) and distribution) of licensed works (an obligation on the part of the producers),
- while meeting fairness expectations (an obligation on the part of both producers and consumers).

How to Pursue Research in Digital Rights?

There are two dimensions to the mechanics of this research.

- One is at a mundane, technological level:
  - To investigate and formalise possible fair use practices,
  - to investigate and formalise rights versus obligations,
  - to investigate and formalise proposed digital rights and obligations license languages such as license and usage languages for "patient medical records" (as documents) and "public administration documents" in their fullest generality,
  - to investigate and formalise wider issues related to digital rights and obligations,
  - to build theories of around all of these, by, for example,
  - reformulating these in possible game theoretic terms.
- The other research dimension is at a combined computer and social sciences level:
  - To investigate and formalise specific "digital rights & obligations" management architectures, and
  - to "lift" these theoretically.

How are we Doing "all" This?

- There is a tightly knit four person core group (Y. Arimoto, D. Bjørner, X. Chen and J. Xiang).
- The group is backed up by Prof. K. Futatsugi, and Assoc. Profs. K. Ogata and R. Vestergaard.
- We will first study the literature.
- We will reformulate formalisations in the literature in CafeOBJ.
- Based on this we expect to formulate new theses, new license paradigms (also in the light of fair use), etc.
- We will analyse and form theories of our reformulations as well as about new theses and paradigms etc.
- We will constantly be relating all of this to issues of game theory.

Consult Our Home Page

- http://www.ldl.jaist.ac.jp/drcp/

拠点形成に関連する主な業績

[1] Dines Bjørner. Software Engineering, Vol. 1: Abstraction and Modelling. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.
[2] Dines Bjørner. Software Engineering, Vol. 2: Specification of Systems and Languages. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.
[3] Dines Bjørner. Software Engineering, Vol. 3: Domains, Requirements and Software Design. Texts in Theoretical Computer Science, the EATCS Series. Springer, 2006.

特任助教授
緒方　和博
OGATA, Kazuhiro
http://www.jaist.ac.jp/~ogata

研究グループ
電子社会のための形式検証技術

専門分野
コンピュータソフトウェア

拠点形成における研究テーマ
ドメインモデルの形式記述と検証

研究の目指すもの

情報技術の発達に伴い、小説、音楽、映画などを代表とする作品が電子化されてきた。また、パーソナルコンピュータの普及により、利用者は電子化された作品（デジタルコンテンツ）を品質の劣化なしにいくらでも複製できるようになった。さらに、インターネットやファイル共有技術の発達と普及により、複製したデジタルコンテンツの利用者間（あるいは流通事業者と購入者間）での送受信や不特定多数の利用者間での共有を可能とした。

このようなデジタルコンテンツの送受信や共有は我々の生活を豊かにする反面、デジタルコンテンツの著作権者が本来享受すべき利益を損なう恐れもある。このため、デジタルコンテンツの健全な流通を促進するための技術が提案され、実際に利用されつつある。そのような技術を総称してデジタル著作権管理（Digital Rights Management；DRM）と呼んでいる。アップルコンピュータ社により運営されている有料音楽配信サービスであるアイチューンズ・ミュージック・ストア（iTunes Music Store；iTMS）では音楽ファイルのCDへの無制限の書き込みを禁止する等のDRMを用いている。

DRMは、デジタルコンテンツの健全な流通にとって不可欠な技術であるのみならず、21世紀の高度情報化社会の健全な発展にも少なからず影響をおよぼすと思われる。このため、DRMが意図どおりの機能を有していることを確認したり、DRMの有すべき基本的な機能とは何かを明確にしたりすること（DRMのドメインモデルの作成、形式記述および検証）は非常に大切なことであると考える。そこで、本研究では以下のようなことを行う予定である。

①既存のDRMを理解し、DRMの（ドメイン）モデルを作成する。
②DRMのモデルを形式仕様言語CafeOBJで記述する。
③DRMのモデルが意図どおりの機能を有していることをCafeOBJ処理系支援のもとで確認（検証）する。
④作成したモデルを基に、DRMの有すべき基本的な機能を明確にし、DRMのモデルを発展させる。
⑤上記②～④を繰り返し行う。

上記④では、特にデジタルコンテンツの購入者・利用者の立場にたったDRMの基本的な機能を明らかにすることに特に力点を置く。というのは、これまでのDRMは、著作権者や流通事業者の利益の保護に力点がおかれているからである。たとえば、これまでのDRMでは公正使用（fair use）を認めるようにはなっていない。しかし、公正使用の解釈は国により異なるため、このような差異をうまく扱えるようなモデルを作成する必要もある。

本研究は、研究チーム「Domain Engineering and Digital Rights Group」で進めている研究プロジェクト「Digital Rights: Consumers and Producers in a Ditital World」（http://www.ldl.jaist.ac.jp/drcp/）の一環として行う。

拠点形成に関連する最近の研究テーマと成果

研究テーマ：OTS/CafeOBJ法：システムの振舞のモデル化、仕様記述および検証

経過と成果：観測遷移機械（Observational Transition Systems：OTSs）でシステムの振舞をモデル化し、モデルを代数仕様言語CafeOBJで記述し、モデルが望みの要件あるいは性質を満たしていることの検証をCafeOBJ処理系支援のもとで行う方法についての研究を行った[1]。観測遷移機械とCafeOBJは以下のような特徴を有している。

●観測遷移機械：
システムを構成するデータや部品の値が時間の経過とともにどのように変化するかに着目してシステムの振舞をモデル化できる。（条件付）等式で自然に記述できる。
図1に示すtest&setを用いた相互排除プロトコルMutexは、図2に示す観測遷移機械S_{Mutex}でモデル化できる。

図1：test&setを用いた相互排除プロトコルMutex

```
Loop
  l1: repeat until ¬ test&set (True, locked);
      Critical Section;
  cs: locked := False;
```

図2：Mutexの観測遷移機械S_{Mutex}

$S_{Mutex} = < O_{Mutex}, I_{Mutex}, T_{Mutex} >$
$\cdot O_{Mutex} = \{ locked : \Upsilon \rightarrow Bool, pc_{i:Pid} : \Upsilon \rightarrow Label \}$
$\cdot I_{Mutex} = \{ \upsilon \mid locked(\upsilon) = False \wedge \forall i:Pid.(pc_i(\upsilon) = l1) \}$
$\cdot T_{Mutex} = \{ enter_{i:Pid} : \Upsilon \rightarrow \Upsilon , leave_{i:Pid} : \Upsilon \rightarrow \Upsilon \}$
If $locked(\upsilon) \wedge pc_i(\upsilon) = l1$, then
  $locked(enter_i(\upsilon)) = True$
  $pc_j(enter_i(\upsilon)) = (\textbf{if } i = j \textbf{ then } cs \textbf{ else } pc_j(\upsilon))$.
If $pc_i(\upsilon) = cs$, then
  $locked(enter_i(\upsilon)) = True$
  $pc_j(enter_i(\upsilon)) = (\textbf{if } i = j \textbf{ then } cs \textbf{ else } pc_j(\upsilon))$.

● CafeOBJ：
理解が比較的容易な（条件付）等式を用いてシステムの仕様を記述し、等式を左から右への書換規則とみなした簡約（による等式推論）でシステムの検証を行うことができる。このため、他の既存の高階論理に基づく証明支援系と比較し、習得が容易であり、検証も見通しの良いものになると考えている。
図３に SMutex の CafeOBJ 仕様を示す。SMutex が満たすべき性質の一つは相互排除性であり、以下の CafeOBJ の項で表すことができる。

```
(pc(S,I) = cs and pc(S,J) = cs) implies (I = J)
```

ここで、S は任意の状態、I と J は任意のプロセス ID である。SMutex がこの性質を満たすことを、CafeOBJ の書き換えの機能を用いて検証することができる。検証の一部を以下に示す。

```
open ISTEP
  op k : -> Pid .
  eq locked(s) = false .  eq pc(s,k) = l1 .
  eq i = k .  eq j = k .
  eq s' = enter(s,k) .
  red istep1(i,j) .
close
```

図３：SMutex の CafeOBJ 仕様

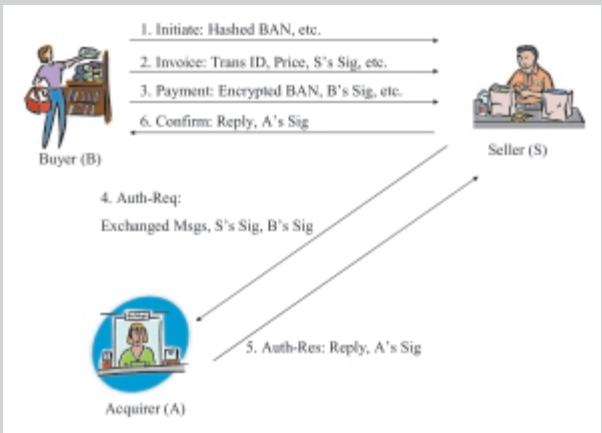
```
mod! MUTEX {
  pr(PID + LABEL)
  *[ Sys ]*
  op init : -> Sys
  bop locked : Sys -> Bool
  bop pc : Sys Pid -> Label
  bop enter : Sys Pid -> Sys
  bop leave : Sys Pid -> Sys
  var S : Sys    vars I J : Sys
  eq locked(init) = false .
  eq pc(init,I) = l1 .
  ceq locked(enter(S,I)) = true if not(locked(S)) and pc(S,I) = l1 .
  ceq pc(enter(S,I),J)   = if I = J then cs else pc(S,J) fi
                           if not(locked(S)) and pc(S,I) = l1 .
  ceq enter(S,I)         = S if not(not(locked(S)) and pc(S,I) = l1) .
  ceq locked(leave(S,I)) = false if pc(S,I) = cs .
  ceq pc(leave(S,I),J)   = if I = J then l1 else pc(S,J) fi
                           if pc(S,I) = cs .
  ceq leave(S,I)         = S if not(pc(S,I) = cs) .
}
```

研究テーマ：OTS/CafeOBJ 法の適用事例：電子商取引プロトコルの検証

経過と成果：電子商取引プロトコルが望みの要件あるいは性質を満たしていることを OTS/CafeOBJ 法を用いて検証した。

1. iKP（i = 1,2,3) の検証：
   iKP は、90 年代に IBM で設計されたクレジットカードによる支払いにもとづく電子支払いプロトコルである（図４）。SET（Secure Electronic Transaction）の設計に影響を与えたプロトコルの一つである。2KP と 3KP が支払合意性「銀行が支払いを認めた場合、それにかかわる買い手と売り手は共にその支払いに合意している」を満たしていることの検証中に反例を発見し、改善案を提案し、改善案が支払い合意性を満たしていることを検証した [2]。
2. TLS（Transport Layer Security）の検証：
   TLS は、IETF（Internet Engineering Task Force）の RFC 2246 で規定されているセキュリティプロトコルで、ウェッブブラウザで採用されている SSL（Secure Socket Layer）の後継である。TLS が望みの要件あるいは性質を満たしていることを検証した [3]。TLS は、考慮した要件をすべて満たしていることがわかった。

図４：iKP 電子支払いプロトコル



iKP と TLS に加え以下の電子商取引プロトコルの検証も行った。

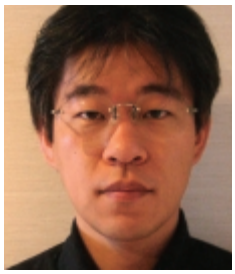
3. NetBill：90 年代に CMU で設計された電子少額支払いプロトコル [4]。
4. Horn-Preneel ：90 年代に欧州で設計された電子少額支払いプロトコル [5]。
5. SET：90 年代に Visa と MasterCard により設計された電子支払いプロトコル [6]。

拠点形成に関連する主な業績

主要論文

[1] Kazuhiro Ogata and Kokichi Futatsugi: Proof Scores in the OTS/CafeOBJ Method, Proceedings of the 6th IFIP WG6.1 International Conference on Formal Methods for Open Object-Based Distributed Systems (6th FMOODS), LNCS 2884, Springer, pp.170-184 (2003).
[2] Kazuhiro Ogata and Kokichi Futatsugi: Formal analysis of the iKP electronic payment protocols, Proceedings of the 1st International Symposium on Software Security (1st ISSS), LNCS 2609 (Hot Topics, Software Security - Theories and Systems), Springer, pp.441-460 (2003).
[3] Kazuhiro Ogata and Kokichi Futatsugi: Equational Approach to Formal Analysis of TLS, Proceedings of the 25th International Conference on Distributed Computing Systems (25th ICDCS), IEEE Computer Society Press, pp.795-804 (2005).
[4] Kazuhiro Ogata and Kokichi Futatsugi: Formal Analysis of the NetBill Electronic Commerce Protocol, Proceedings of the 2nd International Symposium on Software Security (2nd ISSS), LNCS 3233, Springer, pp.45-64 (2004).
[5] Kazuhiro Ogata and Kokichi Futatsugi: Formal verification of the Horn-Preneel micropayment protocol, Proceedings of the 4th International Conference on Verification, Model Checking, and Abstract Interpretation (4th VMCAI), LNCS 2575, Springer, pp.238-252 (2003).
[6] Kazuhiro Ogata and Kokichi Futatsugi: Equational Approach to Formal Verification of SET, Proceedings of the 4th International Conference on Quality Software (4th QSIC), IEEE Computer Society Press, pp.50-59 (2004).

安心電子社会研究センター



特任助教授
青木　利晃
AOKI, Toshiaki
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00060soj.html

研究グループ
電子社会のための形式検証技術

専門分野
ソフトウェア科学・工学

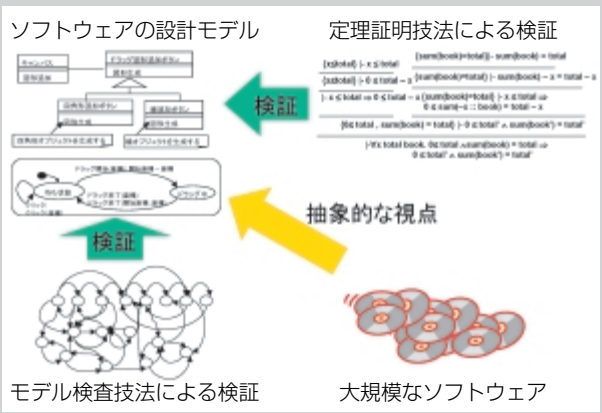
拠点形成における研究テーマ
ソフトウェア設計モデルの形式化と検証

研究の目指すもの

今日の社会には様々なところにソフトウェアが使われており、今後の社会の発展、および、安心した生活を送るためには、正しいソフトウェアを開発する方法を研究することが重要である。そのための１つのアプローチは形式的手法・検証を用いてソフトウェアの正しさを保証することである。一方、社会を支えるソフトウェアは非常に大規模なものであり、かつ、様々なコンポーネントを用いて構成されている。よって、ソースコードの一行一行を検証するというよりは、ソフトウェアの全体の構成について検証することが現実的である。そこで、本研究では、ソフトウェアの設計モデルの形式化を行い、その正しさを検証する手法を提案する。現在、検証技法として、定理証明技法とモデル検査手法が有望視されている。そこで、これらの検証技法をソフトウェアの設計モデルの検証に応用する。

モデル検査技法と定理証明技法

モデル検査技法では、有限状態で特徴づけられる振る舞いを自動的にすべて探索し、不具合を発見する。不具合が発見された場合には、その状況へ導く実行列、すなわち、反例を出力する。定理証明技法では、述語論理などの形式的体系を用いた証明を行う。そのため、本質的に無限の状態を含むものを取り扱うことができ、記述能力が高い。



拠点形成に関連する最近の研究テーマと成果

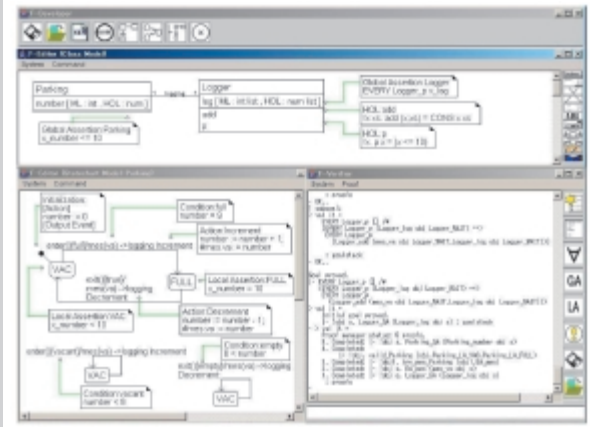
（1）UML により記述された設計モデルの検証法

現在、UML（Unified Modeling Language）と呼ばれるグラフィカルな記法を用いて設計モデルを作成するのが標準になりつつある。そこで、UML で記述された設計モデルを定理証明システムを用いて検証する手法を提案した。設計モデルは定理証明システムで取り扱い可能な形式に変換し、開発者がそのシステム上で検証すべき性質を対話的に証明する。記述能力や検証効率を評価するため典型的な設計であるデザインパターンの検証を行った。その結果、提案手法が十分な記述能力を持っていること、および、効率的に検証できることがわかった。さらに、記述した設計モデルを実行したり、提案した手法に基づいた検証を支援する計算機支援環境を実装した。現在は、検証効率をさらに向上させるために、検証結果を再利用しながら正しい設計モデルを作成する手法について研究を行っている。

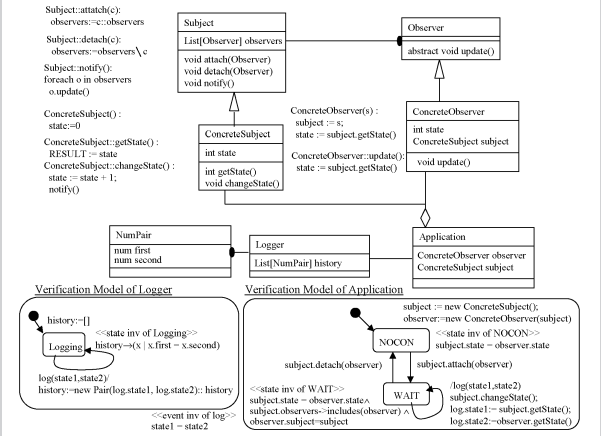
UML（Unified Modeling Language）

UML は OMG（Object Management Group）によって標準化されたオブジェクト指向モデリングのための記法である。静的な側面を記述するためのクラス図や動的側面を記述するためのステートチャート図など様々な記法が定義されている。最近では、OCL（Object Constraint Language）やアクション言語により制約や詳細な動作を記述することができる。しかしながら、厳密性に欠けるため、検証を行うためには形式化を行う必要がある。本研究では、UML の形式化を行い、定理証明システムで取り扱えるようにした。

計算機支援環境



デザインパターン：Observer パターンの記述



(2) モデル検査技法による組込みソフトウェアの検証

組込みソフトウェア開発ではμITRONのような優先度付きマルチタスクが扱えるRTOS（RealTime Operating System）を用いる場合が多い。この場合、並行処理を直接的にプログラムできるが、その反面、その動作の検証が困難になる。並行動作するタスクの実行タイミングを考慮しなければならないからである。このような振る舞いの検証はモデル検査技法が得意とするところである。モデル検査技法を用いると、有限状態で特徴づけられる振舞を網羅的に探索し、デッドロックや飢餓状態などの望ましくない性質を自動的に検出できる。そこで、モデル検査技法を用いてRTOSに基づいたソフトウェアを検証する手法を提案した。本研究では、μITRONに基づいたソフトウェアを対象とした。モデル検査ツールはSpinを用いた。一方で、Spinではタスクのスケジューリングや優先度、その他のサービスコールを直接的には扱うことができない。そこで、それらを扱えるようにするためのライブラリを実現した。これにより、μITRONのサービスコールを直接的にSpinの入力に記述できるようになった。今後は、実際の組込みソフトウェアの検証、および、μITRONに準拠したRTOS自体の検証を行う予定である。

組込みソフトウェア

組込みソフトウェアは通信端末、家電機器、自動車など様々な製品に組み込まれており、今日の社会生活に欠かせない構成要素となっている。そのため、組み込みソフトウェアの誤りは日常生活や経済活動を混乱させ、莫大な時間的、金銭的損失を引き起こす可能性があり、高い信頼性を実現しなければならない。

ライブラリを用いた優先度逆転問題の記述

```
#define P1  1
#define P2  2
#define P3  3
proctype low() provided (turn == P1) {
  do
  :: wai_sem(0,P1)->printf("P1¥n");
     sig_sem(0)
  od}
proctype mid() provided (turn == P2){
  do
  :: printf("P2¥n");
  od}
proctype high() provided (turn == P3){
  do
  :: wai_sem(0,P3);printf("P3¥n");
progress: sig_sem(0); yield(P1)
  od}
init{
  ini();
  cre_tsk(1,P1);
  cre_tsk(2,P2);
  cre_tsk(3,P3);
  cre_sem(0,1);
  sta_tsk(P1);
  sta_tsk(P2);
  sta_tsk(P3);
  run low(); run high(); run mid()}
```

拠点形成に関連する主な業績

主要論文

[1] Toshiaki Aoki and Takuya Katayama, Formalization and Analysis of Dataflow in Object-Oriented Design Models, International Symposium on Object-Oriented Real-Time Distributed Computing 2005, pp.95-105, 2005.

[2] 青木利晃，片山卓也，RTOSに基づいたソフトウェアのためのモデル検査ライブラリ，組込みソフトウェアシンポジウム2005，pp.56-63，2005（優秀論文賞受賞）.

[3]青木利晃，片山卓也，ステートチャートに基づいたオブジェクト指向設計モデルの検証，ソフトウェア工学の基礎ワークショップ， pp.55-64, 2005.

情報科学研究科

教授
落水　浩一郎
OCHIMIZU, Koichiro
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00034soj.html

研究グループ
電子社会のためのモデル化技術

専門分野
ソフトウェア工学

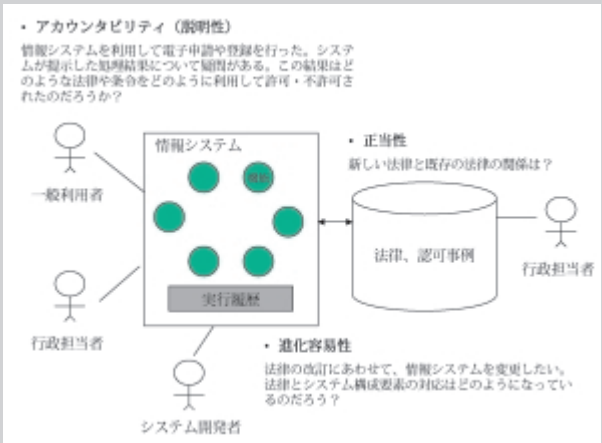
拠点形成における研究テーマ
電子社会におけるアカウンタビリティと
進化容易性の定義と実現

研究の目指すもの

電子社会における情報システムには様々な利害関係者が関与する。例えば、図１に示すように、地方自治体システムの場合、県や市の担当者が新しい法律の制定をはかる際、当該法律の内容のみならず、従来の法律との整合性にも関心を持つ。また、システム開発者は法律内容を、開発する情報システムに正確に反映させることに関心を持つ。さらに、そのようなシステムを利用する一般市民は、システムが提供する実行結果に関心を持つ。本研究は、電子社会における安心性要件のうち、アカウンタビリティと進化容易性に関して、以下に示すような機能を提供するための理論と実現方式の開発を目標とする。

▶アカウンタビリティ：様々な利害関係者からの質問に、彼等のセマンティクスと言語を利用して、システムが答え得る機能。
▶進化容易性：法律の改定に対応して適切に進化できる情報システムの構造。および、それらの進化を支援する機能。

図１



正当性については、電子社会の安心性要件の検証グループ（法推論自然言語処理、法推論機構）によって研究が進められている。本研究では、アカウンタビリティに関しては
・上記グループによって検証済みの法律を対象にして、アカウンタビリティ実現のための知識ベースの開発（自己説明モジュール）
・自己説明モジュールを既存の情報システムに接続できるソフトウェアアーキテクチャの開発
を目指す。進化容易性に関しては、ソフトウェア工学の分野で研究されてきた、変更や進化が容易なソフトウェア構築法を基に、法律とシステム構造の対応に関するアカウンタビリティ機能を提供することで達成する。

拠点形成に関連する最近の研究テーマと成果

（1）原因結果グラフをもちいたアカウンタビリティ知識ベースの設計

本学の履修規則、および、ある会社の社内規定（旅費規程、就業規則、給与規定）を対象にして、原因結果グラフの手法を用いて、規則に従ってある決定を下す際の因果関係を解析した。それを決定表として形式化することにより、自己説明モジュールの設計手段を明らかにした。

適用事例

（1）大学の履修規則には、大学の教育理念に基づいて、修了のための資格が定義されており、また、資格を得るために必要な様々の条件とその修得法が示されている。教員、事務員、学生などの利害関係者が関与する。
（2）会社の社内規定には、運営方針に従った、様々な決定の基となる規則が定められている。管理者、担当者、従業員などの利害関係者が関与する。

C9　：I216の講義の単位を取得済み
C13：I222の講義の単位を取得済み
C45：博士前期課程の学生である
C38：副テーマの研究が終了している
C22：基幹・専門講義科目から５科目以上、導入・基幹・専門講義科目から４分野８科目16単位以上取得している。
C39：研究計画の内容が十分である。

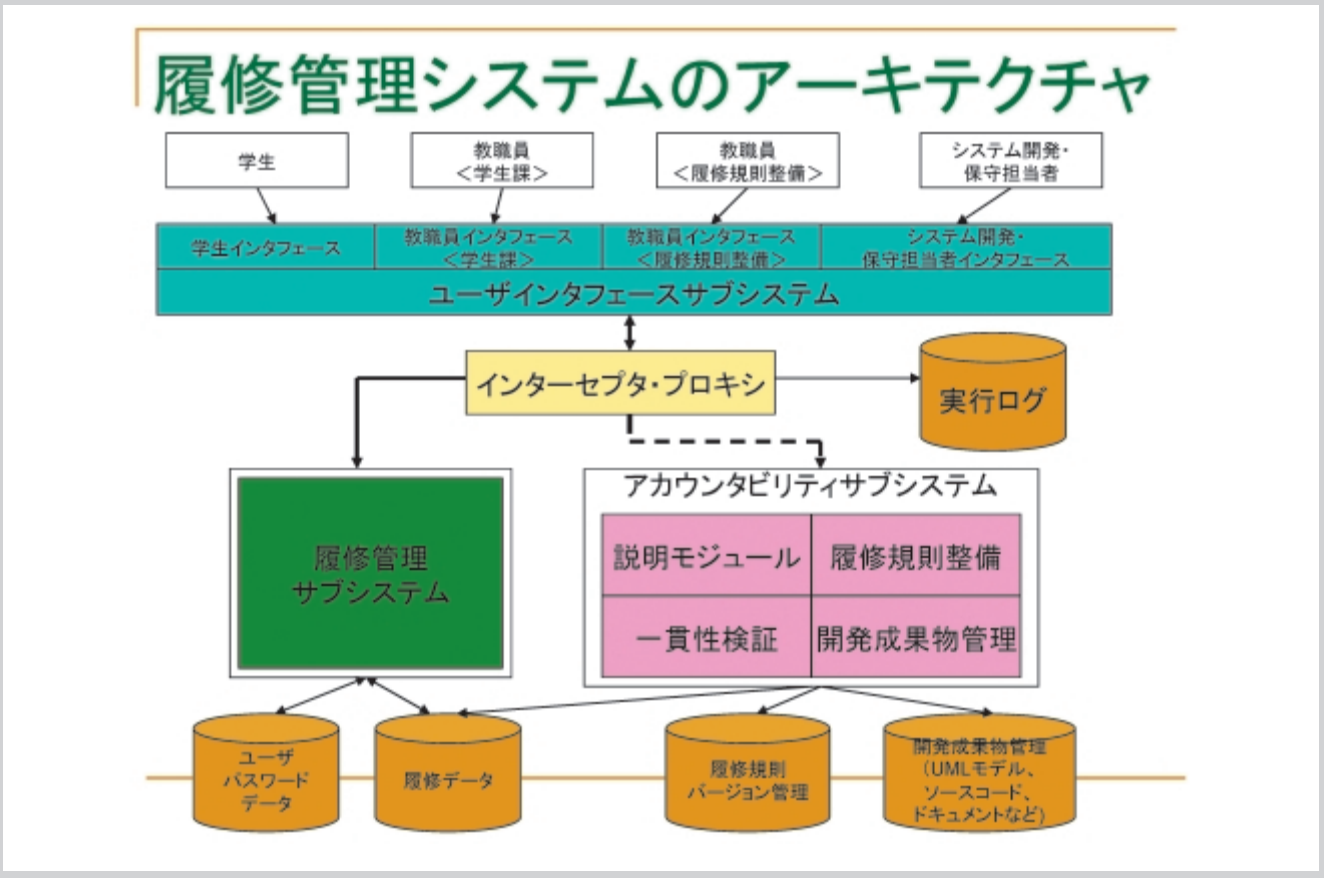
E1　：I431を受講できる　　(C9 | C13) & C45
E33：研究計画書を提出可能である
C45 & C38 & C22 & C39

(2) 自己説明モジュールを容易に接続可能なソフトウェアアーキテクチャ

アカウンタビリティ機能を有するソフトウェアアーキテクチャを定義した。設計上の主眼点を以下に示す。

1. Law-defined system を対象とする。国や地方自治体、会社などの各組織が定める各種規則を社会規則と呼ぶ。社会規則を完全に満たすように構築され、それを確認する手段を提供し、社会規則の変化に応じて迅速に進化させうる情報システムを Law-defined System と呼ぶ。
2. アカウンタビリティ機能の付加は、システムを新たに構築するのではなく、既存のシステムに付加する形で実現できること。
3. 図２において、ユーザインタフェースサブシステムおよび履修管理サブシステムは、電子自治体システムのアーキテクチャとしてよく利用されるアーキテクチャである３層モデルとして設計されている。これにより、既存のシステムに大きく手を加えずにアカウンタビリティ機能を付加するための基礎とする。
4. アカウンタビリティサブシステムをインターセプタ・プロキシによってシステムに結合する。インターセプタ・プロキシは、ユーザインタフェース・サブシステムと履修サブシステムの間での通常の処理をサポートすると共に、ユーザから履修管理サブシステムに渡された処理要求と、返される処理結果に関して、実行履歴を記録する。
5. ユーザインターフェース・サブシステムより実行結果の根拠について問合せがあった場合、システムは実行履歴を手掛かりにして、説明モジュールより、対応する説明を取り出し、ユーザインタフェースに返す。

図２



拠点形成に関連する主な業績

主要論文

[1] 早坂 良，藤枝 和宏，落水浩一郎，“履修管理システムにおけるアカウンタビリティおよび進化容易性を実現するソフトウェアアーキテクチャ”，電子情報通信学会ソフトウェアサイエンス研究会，信学技報 SS2005-32, pp.49-54, 2005.08.
[2] 早坂 良，藤枝 和宏，落水浩一郎，“アカウンタビリティおよび進化容易性を持つ履修管理システムの設計”，日本ソフトウェア科学会 第 22 回大会，CD-ROM, 2005.09.
[3] 金旭東，早坂良，小谷正行，落水浩一郎，“メタパターンを用いた Java ソースコードにおける協調クラス群の抽出”，情報処理学会ソフトウェア工学研究会 , 2005-SE-150, pp.101-108, 2005.
[4] 早坂良、堀雅和、藤枝和弘、落水浩一郎，“アカウンタビリティおよび進化容易性を持つソフトウェアアーキテクチャと３層モデルの対応”，情報処理学会ソフトウェア工学研究会 , 2005-SE-150, pp.1-8, 2005.
[5] 早坂良，落水浩一郎，“履修管理システムにおけるオントロジを用いたアカウンタビリティ設計手法”，情報処理学会ソフトウェア工学研究会 ,2005-SE-151, pp.73-80, 2006.

知識科学研究科

教授
池田　満
IKEDA, Mitsuru
http://www.jaist.ac.jp/ks/labs/ikeda/index.html

研究グループ
電子社会のためのモデル化技術

専門分野
オントロジー工学に基づく知識モデリング

拠点形成における研究テーマ
電子社会進化のための知識体系化

研究の目指すもの

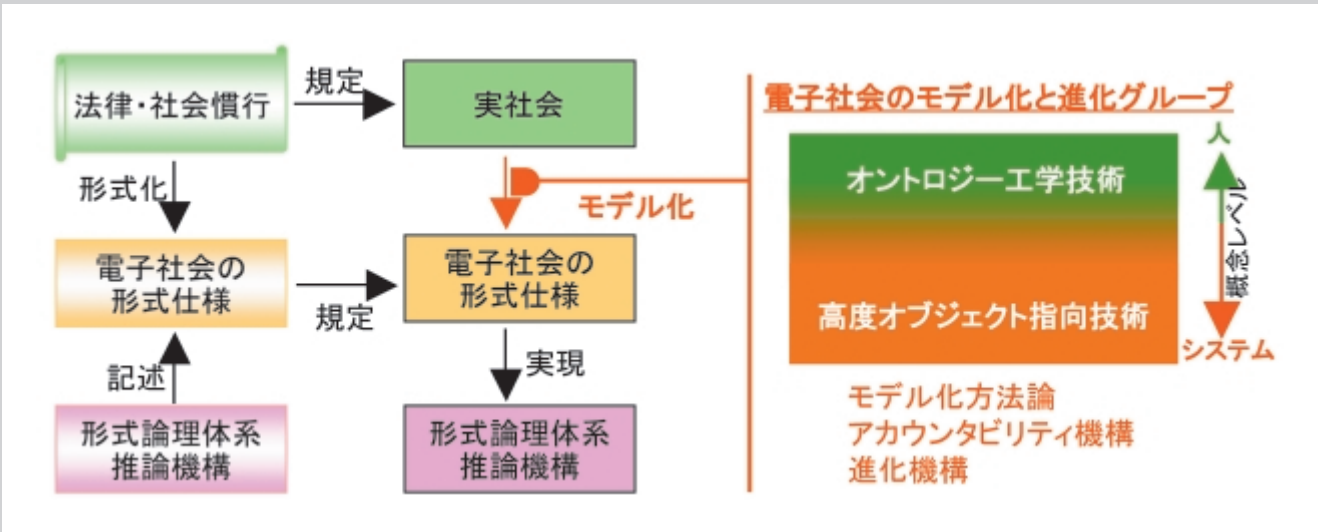
行政・企業の業務は日々変化を遂げている。情報システムはその変化に適切に対応して進化しなければいけない。何が、どのように変化し、それが社会にどのような影響を与えうるのかを明確化し、透明性を確保することが社会的に求められている。このような要求に応えるために、電子社会のモデル化と進化グループでは、知識・業務の変化を適切に捉える概念体系とモデル化手法と、それを情報システムとして適切に実現するための高度オブジェクト指向ソフトウェア開発手法について研究を行っている。本研究テーマでは、前者の課題にオントロジー工学的にアプローチし、電子社会を支える情報システムの安心性を高めるべく、以下の基盤要素技術の開発を目指している。

- ▶ 行政・企業の実業務を構成する概念体系（オントロジー）の構成原理と、それに基づく対象モデル化手法を明らかにする。特に、業務遂行の基礎になる法令・規定を表す概念体系・対象モデルの構成手法、法令・規定の改定を適切に捉えるモデル版管理機構を開発する。
- ▶ 法令・規定モデルに関して、法令・規定間の関係、改訂の影響など、業務関係者による様々な質問に対する説明機構を開発する。
- ▶ 実社会の進化を電子社会システムに適切に反映するために、オントロジー及び対象モデルの改訂と、システムを構成するオブジェクト指向モデルの改訂を整合・同期させる手法とツール群を実現する。

安心基盤技術におけるオントロジー工学の役割（図1）

オントロジー工学の目的は、知識情報処理技術（知識の表現と利用）を適用するにあたり、対象のとらえ方・知識モデルの構成要素・知識モデルを用いた基本的な推論について、知識モデルの利害関係者（知識利用者、知識提供者、システム開発者、システムなど）の間で考え方を共通化し、知識モデルの共有性・再利用性・普遍性を高めることにある。この目的のもとで、オントロジー記述言語処理系、オントロジーの論理的整合性の検証機構、オントロジーマージ・マッピング機構、オントロジー構築方法論などの要素技術の研究が精力的に進められている。本研究拠点では、形式的仕様の推論と検証・法令文書処理・論理検証機構・セキュリティ技術・モデリング技術を高度に密結合させて、電子社会システムの安心性を高めることを目指している。この中で、オントロジー工学は、モデリング技術の一部として重要な役割を担うと考えている。モデリング技術の中では、高度オブジェクト指向技術と社会基盤情報システムに近い位置に、オントロジー工学技術が人間（システム利害関係者）に近い位置にあり、相補的な関係にあると考えられる。本研究課題では、オントロジー工学を基礎として、人間よりの概念レベルで、電子社会のモデル化、アカウンタビリティ、モデルの進化機構に関する安心基盤技術の研究を行う。

図1　安心基盤技術におけるオントロジー工学の役割



拠点形成に関連する最近の研究テーマと成果

オントロジーを基礎にしたモデリング手法の確立と、それを基礎にしたモデル版管理機構について、下記の２つの研究を通じて基礎になる知見を積み上げながら、理論化を進めている。

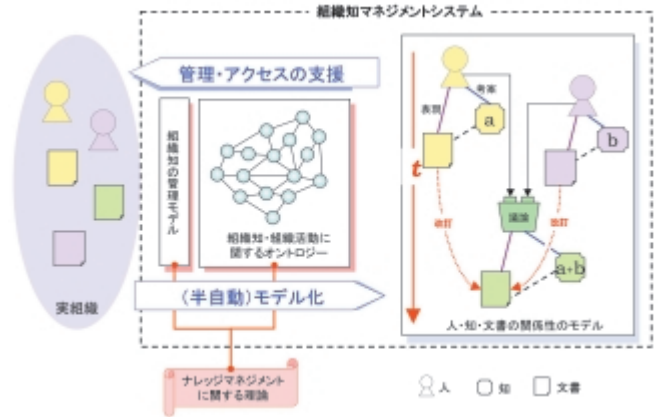
（1）組織知マネジメントシステムに関する研究

組織内の人・知識・文書のモデル化手法を開発し、それを核にした組織知マネジメントシステム（図２）を試作した [1,2]。本研究で得られた知見は以下の３点にまとめることができる。

- ▶ 人の成長・知識の変化・文書の改訂といった、組織知の進化プロセスのモデル化手法。
- ▶ 電子社会における文書管理の基礎になる知識体系（組織知オントロジー）の管理手法。
- ▶ プロセスを重視したナレッジマネジメントの支援手法。

現在、これらの成果を基礎にして、モデルの版管理機構の理論化を進めている。

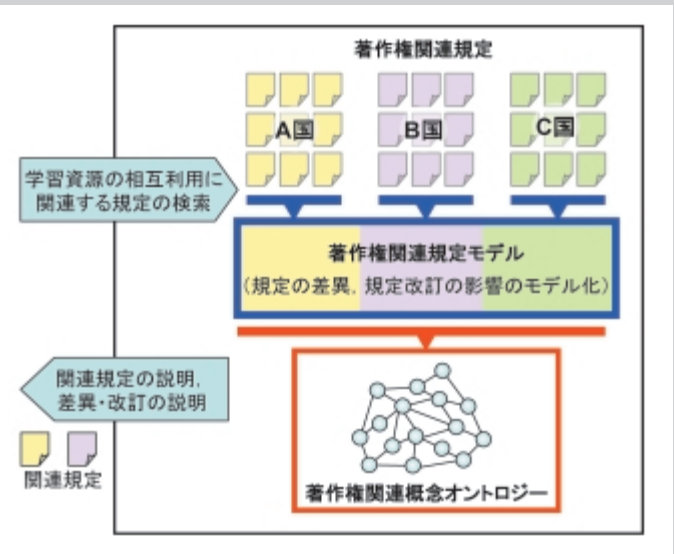
図2　組織知マネジメントシステムの概要



（2）オントロジーに基づく法令のモデリング手法に関する研究

法令の構成概念をオントロジーとして体系化し、法令を表現する知識モデルと推論機構を実装することによって、多様な利害関係者からの質問に答える説明機構の実現を目指している。これまでに、法令文の背後にある目的を法令モデルに顕在化することによって、法令文間の関係性に関する推論機構・説明機構を高度化できることを、事例研究を通じて示している。

図3　e-Learning関連著作権コンサルティングシステムの概要



事例研究

e-Learning コンテンツの著作権規定のモデル化に関する研究 [3]

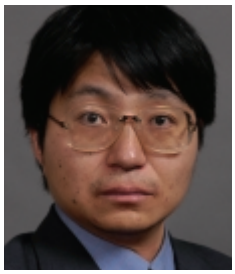
e-Learning 技術の普及が進み、学習コンテンツの国際的な相互利用に向けて様々な試みが進められている。しかし、著作権法に関する諸規定は国ごとに異なり、また改訂が頻繁になされるため、e-learning 関係者（システム開発者・運用者・コンテンツ作成者）にとって学習資源を相互利用することが非常に困難になっている。本研究では、適切な著作権関連情報を提供するコンサルティングシステム（図３）を開発し、学習コンテンツの国際的相互運用の安心性を高めることを目指している。これまでに、著作権規定に関わる諸概念のオントロジーと、それに基づいた規定の差異を明確にするモデルが成果として得られており、現在は規定の改定が及ぼす影響を明確にするモデルの構築を進めている。

拠点形成に関連する主な業績

[1] 池田 満，林 雄介，知の創造・継承のモデル化と支援システムのデザイン，ヒューマンインタフェース学会誌・論文誌　学習・創造・インタラクション特集，Vol. 6，No.2，pp. 19-26，2004.

[2]Ikeda, M., Hayashi, Y., etc., Intellect Disclosure Support Based On Organizational Intellect Model,International Semantic Web Conference 2004 Workshop on Applications of Semantic Web Technologies for E-learning, 2004

[3]An Intention-oriented Model of Copyright Law for e-Learning: International Semantic Mapping of Copyright Laws Based on A Copyright Ontology, Lu, W., Ikeda, M., Proceedings of International Conference on Computer and Education 2005, pp.753-756, 2005



助教授
鈴木　正人
SUZUKI, Masato
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00239soj.html

研究グループ
電子社会のためのモデル化技術

専門分野
ソフトウェア工学

拠点形成における研究テーマ
電子社会のためのコンポーネント技術

研究の目指すもの

電子社会では形態、要求の変化に応じた柔軟なサービスの提供が必要になる。これらの要求の中には従来の情報システムで見られる機能追加・変更・修正などの他に、説明可能性（アカウンタビリティ）の実現という新しい概念や原理に基づくものが明らかになりつつある。

一方で、ソフトウェアの機能拡張（進化）のためには古くから多くのモジュール化技術、再利用技術が実用化されている。中でもコンポーネント（部品化）技術は、多様なサービスが必要とされるWEBアプリケーションの分野や、製品の開発期間が短い組込みシステム開発の分野において、再利用性と信頼性を向上させるための基盤技術として注目を集めている。本研究はこれらのコンポーネント技術を、進化可能な電子社会の基盤となる情報システムに適用するために、必要となる要素技術を確立し、説明可能性を実現する基本構成（アーキテクチャ）を導出することを目標とする。

▶ 説明可能性を決定する要因：ドメイン言語により記述された仕様（法律／規則）と情報システム内でのモデル要素との対応関係の明確化

▶ 説明可能性を実現するメカニズム：不変な部分（アーキテクチャ）と可変な部分（コンポーネント）の分離

▶ 従来の情報システムへの説明可能性の導入：アーキテクチャに基づく再構成

図１：従来の情報システム

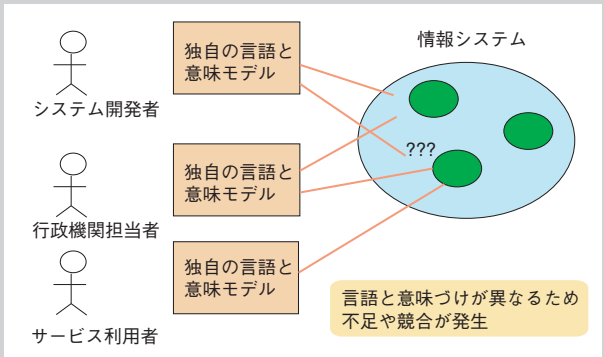
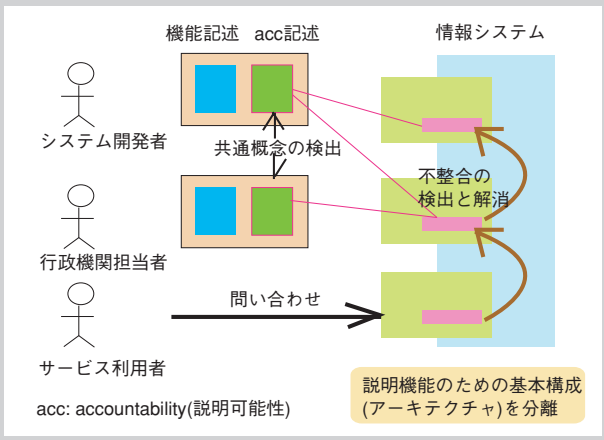


図２：目標とする情報システム



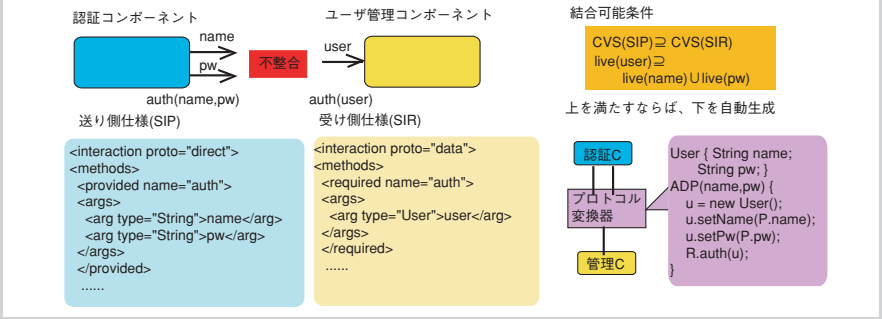
拠点形成に関連する最近の研究テーマと成果

（1）コンポーネントの整合性検証と不整合の解消

コンポーネントを利用した開発ではまずアーキテクチャを決定し、機能要求を実現する複数のコンポーネント（部品）を組み合わせて情報システムを構成するのが一般的である。現在はコンポーネントが様々なベンダから提供されており、各ベンダが独自の概念モデルやデータドメインに基づいているため、利用者は自分が必要とする機能がそのコンポーネントで実現可能か判断するのが困難であり、同一機能のコンポーネントでもベンダ間で互換性がない、また複数のコンポーネントを組み合わせる際に、データ型（ドメイン）やデータ通信形態（プロトコル）が異なるため同時利用ができない、といった問題が発生している。複数のコンポーネントを同時利用し情報の授受を確実に行う（＝結合）際に、従来は情報の送信側、受信側の関数の単位で引数の数と型（＝シグネチャ）が一致していない限り送受信が不可能であった。

本研究ではコンポーネントの仕様として関数単位のシグネチャに加えて、ベンダ独自のデータドメインを記述し、部分型比較を行うことで整合性検証を可能としている。またプロトコルの単位での仕様記述を付加することで、関数単位のシグネチャが不整合であった場合でも結合を可能とする条件を特定、それに基づいた検証と、不整合を解消するためのプロトコル変換器（＝アダプタ）の生成を半自動的に行う（図３）。

図３：プロトコル不整合の例とその解消



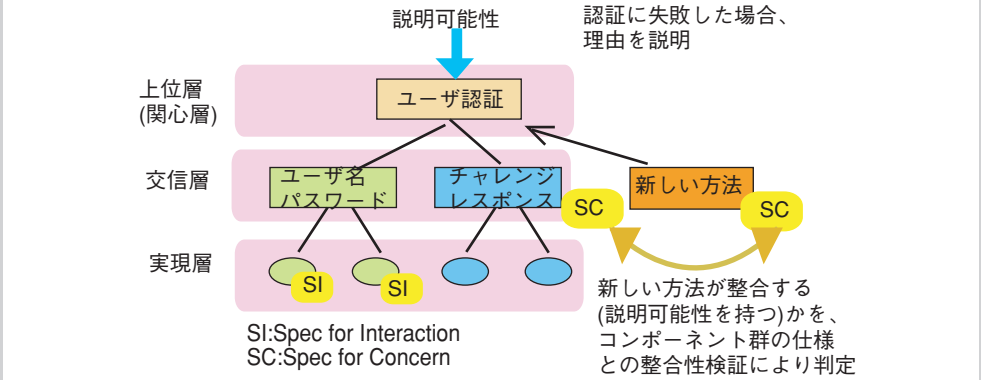
(2) 説明可能性を実現するためのコンポーネント群の仕様記述

（1）では関数単位の仕様記述にプロトコル単位の記述を付加することにより、実現は異なるが交信の意味付けが等しいコンポーネント間の結合可能性を向上させている。この考え方をより上位の層に拡張することで、説明可能性とそれを実現するためのコンポーネント仕様記述の方法を提唱する。

情報システムにおける各利害関係者は異なった言語および概念モデルに基づいて仕様を記述（理解）しているため、同一の機能／非機能要求であるにもかかわらず異なった表現を持つ場合が多い。利用者の説明要求を上位層の仕様と捉えると、説明要求を実現する複数の構成要素間における交信（インタラクション）が交信層に記述されていると考えることができる。現在コンポーネントはそれぞれ単一の交信の仕様（＝プロトコル）を実現するものとして実装されているが、複数のコンポーネントを対象として交信層の仕様を付加することで同一の上位層への整合すなわちある説明要求に対する実現性の有無（＝整合性の検証）、および実現性がない場合にはそれを持たせるための条件（＝不整合の解消）の発見を可能にする。これにより新しいコンポーネントに関しても説明可能性を実現することが可能になる（図４）。

また説明可能性は複数の構成単位に影響を与える要因（横断的関心事項）と考えることができる。上位層と交信層の仕様を完全に分離して記述するのではなく、上位層の複数の要素が交信層に影響を与える場合にそれぞれを関心（アスペクト）として表現するための関心点（ポイントカット）や処理内容（アドバイス）の記述方法を確立する。

図４：コンポーネント群の仕様記述による説明可能性の判定



(3) 情報システムのコンポーネントによる再構成

（1）、（2）の成果をふまえて、説明可能性をもつ情報システムが保有すべきメカニズムの導入が容易になるように、既存情報システムを再構成する。最初に情報システムの構成要素（クラス）間の通信形態を抽出、分類し、コンポーネントとして分離可能な部分を決定する。コンポーネントは単一のクラスと比較してインターフェースが確立されている、インターフェースを自由に拡張できるといった特徴があるが、分離した構成要素（群）のうち、説明可能性の実現のためにインターフェース修正が必要な部分を決定し、実際にインターフェースを拡張する。その際に従来の技術における機能単位の拡張のみでなく、アスペクトを考慮した拡張の方法を確立する。

コンポーネントを分離した後、説明可能性の実現に普遍的な構造をフレームワークとして定義し、抽出したコンポーネントをフレームワークに適合させるためのインターフェースの修正を行う。この再構成により情報システムは再利用性や変更容易性、信頼性が向上すると共に、説明可能性の実現のための基本的なメカニズムとしてのアーキテクチャおよびその進化のための能力を保持することが可能になる。

情報科学センター

教授
篠田　陽一
SHINODA, Yoichi
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00054soj.html

研究グループ
電子社会のための安心基盤技術

専門分野
ネットワーク分散システム

拠点形成における研究テーマ
実践的手法による大規模ネットワークの健全性と安全性の検証

研究の目指すもの

インターネットの存在なくして、ここ数年来の電子化社会への急激な移行は不可能であったと言える。新しいアプリケーションはもちろんのこと、既存の通信システムもがインターネットへの収斂を進め、さらに流通システムや既存ライフラインがインターネットへの依存を深めていくことで、インターネットはすでに電子化社会の超ライフライン的役割を演じ始めているといっても過言ではない。

ところがインターネットは特定の主体が運用する単一のシステムではなく、さらにインターネットを構成するサービスは互いに複雑に関連し合っているという性質は、従来のライフラインとは一線を画すものになっている。従来のライフラインは一般的に言って、その性質が故障時の挙動などを含め、シミュレーションなどを通して良く研究されてきた。これに対してインターネット、あるいはインターネット上のシステムではこのような研究が少ない。

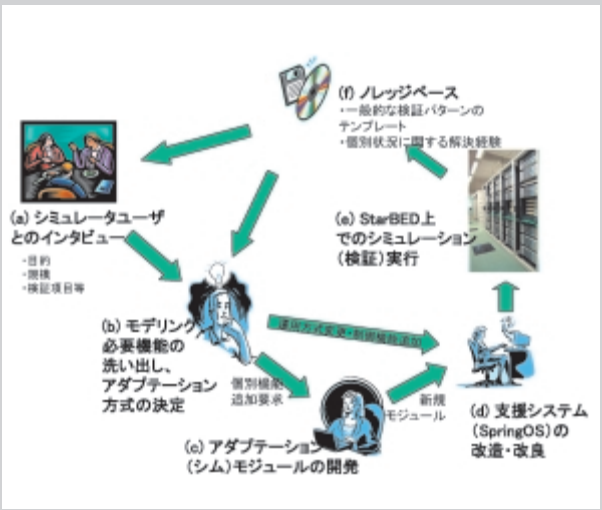
本研究は、比較的大規模なハードウェアシミュレータを使用し、現実的な規模でインターネットそのもの、あるいはインターネット上の複数のシステムをシミュレートすることにより、これらのシステムの健全性や安全性を検証する方法を確立することを目的としている。

拠点形成に関連する最近の研究テーマと成果

（1）実証実験を通したインターネットシステムの検証方法に関する知識習得

高々数十台のノードを使用して研究室規模での研究開発や単機能試験を行う場合と比べ、より現実的な環境で実践的な実証実験を実施するためのハードルは比べ物にならないほど高い。その要因のひとつに、検証方法に関する知識の欠如があげられる。われわれは、主に StarBED インターネットシミュレータ（情報通信機構 /NICT・北陸 IT 研究開発支援センター）を利用した研究開発を行なってきたが、検証に関する知識の蓄積を目的として一般利用者に対し、多数のコンサルテーションを実施してきた（図 1）。この結果は検証方法の確立に反映されると同時に、（2）の検証支援システムの設計と実現に反映された。

図 1 StarBED での検証に関する知識の蓄積



（2） 大規模な実証実験用シミュレータの運用支援システムの開発

何万ものノードを扱うようなシミュレーションでは、実験の準備や実施を人手で行うことは全く非現実的であり、機械的な支援が不可欠である。このような支援を行う、言わばシミュレータの基本オペレーティングシステムの構成法は、それ自身が重要な研究課題である。われわれは、多数の支援ツールの集合からなる検証支援システム SpringOS を実装してこの問題を解決した。SpringOS を構成するコンポーネントの実現には、シミュレータ内のシミュレーションノードを含むさまざまな機器の構成の自動生成と自動設定する仕組み [1] や、ランデブーを用いる制御方式 [5] が用いられている。

(3) 基本シミュレーション方式の拡張

StarBED は基本的に物理ノードをそのままインターネット上のノードに 1 対 1 に対応させてシミュレーションを行なうように設計されたが、この方式ではシミュレーション規模の上限が物理ノード数の上限と一致してしまい、シミュレーションの要求によっては現実的な環境でのシミュレーションが行なえないこともある。そこでわれわれは、シミュレータ内のオブジェクトとシミュレーション対象のオブジェクトの対応関係を多重化係数別に何種類か用意することにした（図 2）。

適当な多重化方式を採用することで、物理的な設備の限界を超える大規模なシミュレーションが可能となる。このうち、VM 多重方式については 4 多重を用いた 1,000 ノードを超える検証経験 [3] があり、VM の制御も SpringOS に組み込まれている [2]。またプロセス多重に関しては、2006 年 2 月に 5,000 シミュレーションプロセス / 物理ノードを用いて StarBED 上で 100 万台オーダのノードをシミュレートすることに成功している。

図 2　シミュレーション方式と多重化係数

多重化方式	シミュレーション内のノードの表現方法	多重化係数（範囲）	多重化係数（実績）
直接対応	物理ノード	1	1
VM多重	仮想マシン(VM)機構で多重化された物理ノード	4-10	4
プロセス多重	プロセス	100 - 5000	5000
スレッド多重	スレッド	500 - 20000	（なし）

(4) 大規模実証実験用シミュレータの広域活用方法に関する研究

StarBED のような大規模実証実験シミュレータは、その汎用性を生かして他の実証実験システムと広域接続することにより、それらの実証実験システムの実験能力を増大させたり、全体として新しい実証実験システムを構成するために用いることができ、規模的にも機能的にも、より多様なシステムの健全性・安全性の検証を行うことを可能にする。これをわれわれはテストベッドのシナジー効果と呼んでいる。

一例として、大規模で現実的な分散サービス妨害攻撃（DDoS）対処方法の検証環境の実現を示す。われわれは、東京の NICT 小金井本部に設置された脆弱性再現装置（SIOS）、NICT 神戸リサーチセンターに設置された小規模汎用テストベッド VM-Nebula、そして StarBED を用いて DDoS 攻撃を現実的な環境で再現することに成功した [4]。もともと SIOS は DDoS 攻撃のシミュレーションを中間ネットワークを省いた形で行なう機能を備えているが、ある種の対応方式では中間ネットワークをシミュレートすることが不可欠である。このシミュレーションでは、SIOS に攻撃者の役割を、StarBED には大規模な中間ネットワークの役割を、VM-Nebula には被害者の役割をそれぞれ割り振ることで中間ネットワークを含んだ現実的なシミュレーション環境が構築できたことになる。

図 3　テストベッド間結合による検証環境

拠点形成に関連する主な業績

主要論文

[1] Toshiyuki Miyachi, Ken-ichi Chinen and Yoichi Shinoda, Automatic Configuration and Execution of Internet Experiments on an Actual Node-based Testbed, Tridentcom 2005, Trento, Italy, ISBN 0-7695-2219-X, pp.274--282, Feb, 2005.
[2] 宮地 利幸 , 知念 賢一 , 篠田 陽一 , SpringOS/VM: 大規模ネットワークテストベッドにおける仮想機械運用技術情報処理学会研究報告書 , 2005-OS-99, pp.105-112, May 2005, ISSN 0919-6072.
[3] Eiichi Muramoto, Takahiro Yoneda, Atsushi Nakamura, Makoto Misumi, Toshiyuki Miyachi and Yoichi Shinoda, Report on a Method of Simulating Multicast Group Communication on the Internet, In Proceedings of the symposium “Towards Peta-Bit Ultra Networks”, Sep. 2003.
[4] 三輪 信介 , 宮地 利幸 , 大野 浩之 , 不正アクセス等再現実験環境の統合実験 , マルチメディア , 分散 , 協調とモバイル（DICOMO2005）シンポジウム論文集 , pp.393-396, ISSN1344-0640, 情報処理学会 , Jul. 2005.
[5] Ken-ichi Chinen, Toshiyuki Miyachi and Yoichi Shinoda, A Rendezvous in Network Experiment --- Case Study of Kuroyuri, TridentCom 2006, Barcelona, Spain, ISBN 1-4244-0106-2, Mar, 2006.

特任助教授
DÉFAGO, Xavier

http://www.jaist.ac.jp/~defago/

研究グループ
電子社会のための安心基盤技術

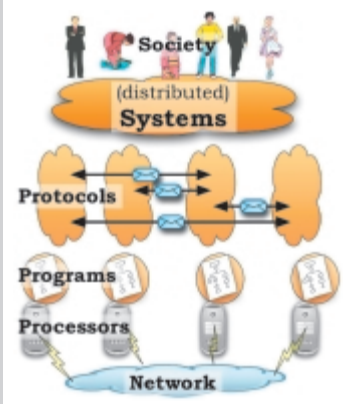
専門分野
分散システム、高信頼性、耐故障性

拠点形成における研究テーマ
電子社会のための高信頼インフラストラクチャー

研究の目指すもの

Our society is becoming gradually more dependent on its global information infrastructure, as evidenced by the widespread reliance on the Internet and related systems (e.g., Grid, e-Government initiative, etc.). In order to provide a verifiable and accountable e-Society, it is hence essential to use an infrastructure on which one can justifiably depend. There are five essential runtime aspects that our communication infrastructure must meet, namely, reliability, availability, security, manageability/evolution, and performance. Our research focuses particularly on the first two aspects, that is, reliability and availability.

A distributed system is a collection of autonomous entities (e.g., computers) that are linked by a communication subsystem (e.g., network), and that cooperate to provide a given service or functionality. The entities must communicate and coordinate their actions, so that users (i.e., society) perceive the whole thing as a single coherent system.



The goal of our research is to provide basic generic mechanisms and protocols to support the development of highly reliable and dependable distributed systems and applications. Our work aims at keeping a balance between the development of sound theoretical results, and practical requirements and assumptions. In particular, we focus on three important issues. First, we develop improved coordination protocols for fault-tolerance in distributed systems such as the Internet. Second, we improve the ability of such systems to detect, with high probability, the crash or misbehavior of some of the computers of the systems. Third, we investigate the question of reliable coordination of entities in the context of mobile systems. More precisely, we consider systems that consist of a large number of mobile nodes for which we need to coordinate the movement, such as, cooperating robots, automatic factories, and intelligent transport systems.

拠点形成に関連する最近の研究テーマと成果

Fault Tolerant Group Communication & Agreement Protocols

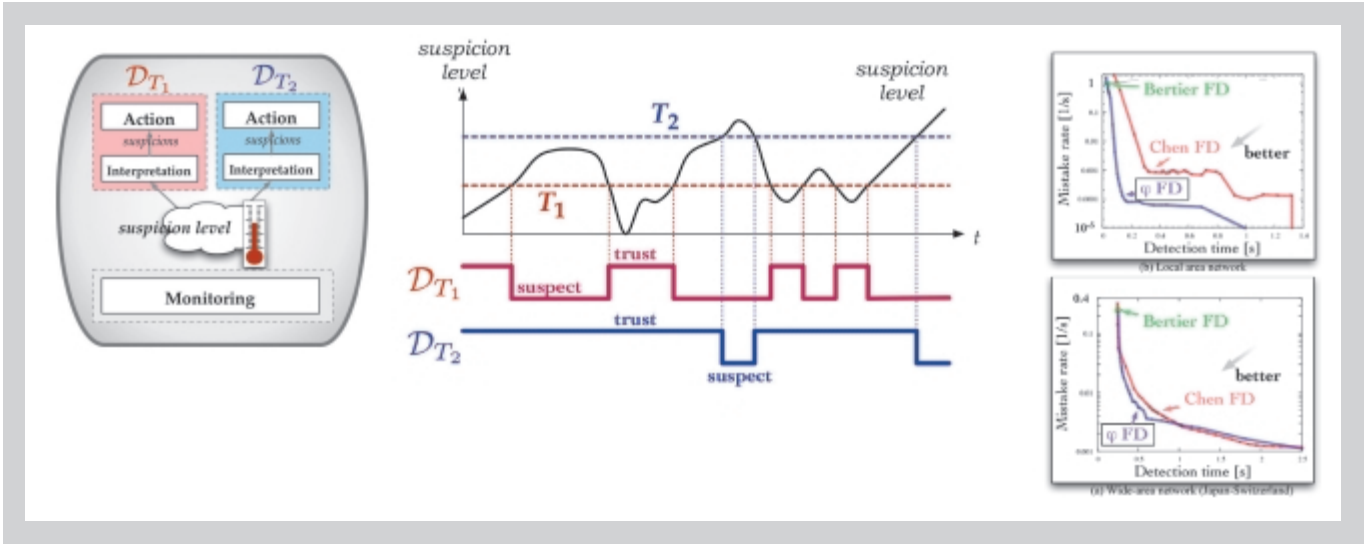
Group communication and distributed agreement are basic primitives to maintain cohesion among a set of participating nodes a distributed system, by allowing them to agree on important issues. Large distributed infrastructures can be seen as a very large collection of interacting services. Agreement protocols are used as a fundamental building block to support the replication of important services, thus improving their availability. Consequently, with a reduction in the downtime of services, the overall reliability and performance of the distributed infrastructure is greatly improved. While group communication and agreement mechanisms can support reliability, they must themselves be able to tolerate faults, by operating even when some of the participants may possibly fail.

Group communication and agreement are strongly related. A very practical instance of agreement is a group communication primitive called *Total Order Broadcast* (also *Atomic Broadcast*). In short, this primitive allows any of the participating nodes to broadcast messages at any time, but ensures that all destinations always deliver (and process) the messages in exactly the same sequence. Provided that they start with the same view of the system, Total Order Broadcast allows the participating nodes to locally reach identical conclusions without requiring any further communication. Our research aims at developing more efficient, scalable, and robust algorithms.

Failure detection

Failure detection plays an essential role in ensuring fault tolerance in a distributed system infrastructure. Our research aims at defining a generic failure detection infrastructure to support the development of fault-tolerant systems on a global scale.

There are three major challenges for creating a generic failure detection service. First, the service must properly



adapt to highly changeable working conditions while simultaneously meeting the potentially stringent requirements of multiple independent applications. Second, the service must be easily deployed, compatible with existing technology, and its interface simple and as close as possible to existing standard. Third, the service must be extremely scalable and self-configuring.

To address the first challenge, we have defined a novel approach to failure detection, called *accrual failure detectors.* This approach replaces the conventional "binary" model of failure detectors (i.e., trust or suspect) with a gradual model expressing a suspicion level. Although simple in principle, the change of model allows for more failure detection that better match the requirements of distributed applications. Concretely, we have been able to formally establish the link with the existing theory, and we have developed several advanced protocols. Experiments have shown that our protocols could improve performance up to tenfold.

To address the second challenge, we are currently developing a prototype service that relies exclusively on existing Internet standard, such as the SNMP protocol. The advantage of this approach is that the use SNMP protocol helps gather more information about failures, while providing an service interface compatible with SNMP makes it easier to use for application developers, as well as allowing the use of the large collection of utility programs available.

To address the third challenge, we need to rely on a self-organizing structure to support mechanisms for the notification and propagation of failure information. Although we develop mechanisms that are provably correct, we need to assess their performance in real working environment.

Autonomous Mobile Systems

With the technological developments of the last decade, mobile systems have gradually become more-and-more integrated in our society. While wired systems are unlikely to disappear, the trend toward mobility is bound to increase, until the vast majority of the society infrastructure will be mostly composed of various kinds of mobile systems, such as mobile stations, sensor networks, mobile robots, or intelligent transport systems. It is therefore essential to anticipate this trend and make sure that we can develop a dependable infrastructure for mobile systems. But, while mobility brings many important new applications possibilities, it also brings very difficult challenges from the perspective of the system.

In our research, we focus on ensuring proper dependability and fault-tolerant mechanisms for mobile systems. We address the problem from both a theoretical and a more pragmatic perspective. On the theoretical side, we investigate the minimal capabilities that the mobile node need to solve a given problem. Especially, we look at the existence of solutions that work even when sensors provide unreliable information. On the pragmatic side, we aim at providing a basic coordinated movement mechanisms whereby mobile nodes are unable to collide against each other, thus forming the basis for a fail-safe system. We make the link between conventional fault-tolerant system, ad hoc networking, and cooperative mobile robotics.

拠点形成に関連する主な業績

Selected Papers

[1] Xavier Défago, Péter Urbán, Naohiro Hayashibara, Takuya Katayama. Definition and specification of accrual failure detectors. In *Proc. Intl. Conf. on Dependable Systems and Networks (DSN),* pp. 206–215 (2005)

[2] Xavier Défago, André Schiper, Péter Urbán. Total order broadcast and multicast algorithms: Taxonomy and survey. *ACM Computing Surveys,* 36(4):372–421 (2004)

[3] Xavier Défago, André Schiper. Semi-passive replication and lazy consensus. *Journal of Parallel and Distributed Systems,* 64(12):1380–1398 (2004)

[4] Naohiro Hayashibara, Xavier Défago, Rami Yared, Takuya Katayama. The ϕ accrual failure detector. In *Proc. 23nd IEEE Intl. Symp. on Reliable Distributed Systems (SRDS),* pp. 66–78 (2004)

情報科学研究科

教授
SHEN, Hong

http://www.jaist.ac.jp/~kkgi/thisyear/soe/00271soe.html

研究グループ
電子社会のための安心基盤技術

専門分野
Networking, Parallel and Distributed Computing, Algorithms, Database Query Evaluation, Data Mining, Multimedia Systems.

拠点形成における研究テーマ
電子社会のための論理シミュレーション技術

研究の目指すもの

(i) Mobile Agents in E-Applications: Study new models, methods and techniques for analyzing statistical behaviors of mobile agents, monitoring agent's performance and controlling agent's activities, to improve the performance of agent-driven e-applications.
(ii) Web Technology: Study effective methods and techniques for Web caching, scalable Web server design, proxy/cache placement and replacement. Recent focuses include development of optimal methods for en-route Web caching in tree networks and multimedia objects placement for transparent data replication.
(iii) Network Topology Discovery and Performance Evaluation: Study effective models, methods and techniques for network traffic analysis and performance management. Recent focuses include network topology (traffic pattern) discovery in Internet, multicast network and wireless networks; network performance analysis and evaluation based on the knowledge in the discovered topologies.
(iv) Optical Computing: Study efficient architectures and algorithms for optical computing, with the focuses on routing in optical WDM networks and design and analysis of optical interconnection networks.
(v) Network Security and Privacy-Preserving Computation: Study effective models, methods and techniques for anomaly-based intrusion detection in hosts and networks with provision of adaptability, scalability, and dependability; for privacy-preserving computation in various applications.
(vi) Parallel Algorithms: Study efficient parallel algorithms for problems ranging from combinatorial and graph-theoretic to data-intensive applications. Recent attention has been drawn to combinatorial problems on partially ordered data sets and critical sections in networks.
(vii) Parallel Databases Query Evaluation and Data Mining: Study efficient techniques and methods for efficient databases query evaluation and data mining in parallel and distributed environments, with the focuses on multiple join operations and discovery of association patterns in large databases.
(viii) Wireless Communication and Networking: Study efficient methods and techniques for wireless communication and networking. Recent focuses include: Design orthogonal and quasi-orthogonal space-time block codes with high rates and low delays; Develop efficient, robust and secure routing protocols for MANET.
(xi) Data hiding, multimedia coding and transmission: Study effective methods and techniques for embedding high-capacity data imperceptibly in a host media (audio, image and video etc) in a robust and secure manner, for error-resilient coding and transmission of multimedia applications in noisy and time-varying network environments.

拠点形成に関連する最近の研究テーマと成果

Performance Analysis for Mobile Agents Deployed Applications: Developed several new models and mathematical analyses for mobile agent execution in network routing and e-commerce.
En-Route Web Caching: Developed optimal methods for caching objects and multimedia objects with transcoding capability in multiple-client-single-server tree structured networks.
Network Topology Discovery: Developed new methods for multicast network topology discovery and network internal performance (link loss and link delay) inference.

Network Security: Developed new schemes applying SVM, multi-variable SP and detectors coordination for anomaly-based network intrusion detection.
Image Coding and Data Hiding: Developed effective methods for image compression and water marking, using wavelet-transform technique with grouping regions by interestingness.
Privacy Preserving Computation: Investigated effective methods for PP vector and matrix operations.
Wireless Networks: Developed effective methods for topology deployment and routing in wireless senor networks. Studied the data gathering problem in WSN.
Routing: Proposed new approximate algorithms for computing edge-disjoint paths.
Optical Networks: Proposed efficient schemes for embedding FFT and hypercube communication patterns onto linear array and mesh optical networks.

拠点形成に関連する主な業績

A. Journal papers

[1] Keqiu Li and H. Shen, "Coordinated En-Route Multimedia Object Caching in Transcoding Proxies for Tree Networks", *ACM Transactions on Multimedia Computing, Communications and Applications* (TOMCAPP), Vol. 1, No. 3, 2005, p. 289-314.
[2] Keqiu Li, H. Shen, F. Chin, and S. Zheng, "Optimal Methods for Coordinated En-Route Web Caching for Tree Networks", *ACM Transactions on Internet Technology* (TOIT), Vol. 5, No. 3, 2005, p. 480-507.
[3] Keqiu Li and H. Shen, "Optimal Methods for Proxy Placement in Coordinated En-Route Web Caching", IEICE Trans. on Communications, Vol. E88-B, No. 4, pp. 1458-1466, April 2005.
[4] Keqiu Li and H. Shen, "Optimal Methods for Object Placement in En-Route Web Caching for Tree Networks and Autonomous Systems", *International Journal of High Performance Computing and Networking* (IJHPCN), Vol. 4, No. 5, 2005.
[5] Haibin Kan and Hong Shen, "A relation between the characteristic generators of a linear code and its dual," *IEEE Transactions on Information Theory*, Vol. 51, No. 3, 2005, p. 1199-1202.
[6] Haibin Kan and Hong Shen, A counterexample for the conjecture on the minimal delay of orthogonal designs with maximal rates, *IEEE Transactions on Information Theory*, Vol. 51, No. 1, 2005, p. 355-359.
[7] Gui Xie and Hong Shen, "Highly Scalable, Low-Complexity Image Coding Using Zeroblocks of Wavelet Coefficients", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, No. 6, 2005, p. 762-770.
[8] Zonghua Zhang and Hong Shen, "Application of Online-training SVMs for Real-time Intrusion Detection with Different Considerations", Computer Communications, Vol.28, No. 12, Elsevier, 2005, p.1428-1442.
[9] Haibin Kan and Hong Shen, Trellis Properties of Product codes, *IEICE Transactions on Fundamentals*, Vol. E88-A, No. 1, Jan. 2005.
[10] Hui Tian and Hong Shen, "Multicast Based Inference for Topology and Network-Internal Loss Performance from End-to-end Measurements", accepted by *Computer Communications*, Elsevier, Dec. 2005.
[11] Hui Tian and Hong Shen, "An improved algorithm of multicast topology inference from end-to-end measurements", accepted by *International Journal of Communication Systems*, John Wiley & Sons, 2005.
[12] Hui Tian, Hong Shen and Teruo Matsuzawa, "Energy-Efficient Topologies and Routing for Wireless Sensor Networks", *GESTS International Transaction on Computer Science and Engineering*, No.1, Vol.8, pp. 79-89, May 2005.
[13] Hui Tian, Hong Shen and Teruo Matsuzawa, "Random Walk Routing for Wireless Sensor Networks", International Journal of Computer Science and Network Security, accepted, 2005.
[14] Ke Deng, Hong Shen and Hui Tian, "Self projecting time series forecast: an online stock trend forecast system", accepted by *International Journal of Computational Science and Engineering*, 2005.
[15] W. Qu, H. Shen and J. Sum, "Stochastic Analysis on Mobile Agent-Based E-Shopping", *International Journal of Electronic Business*, Vol. 3, No. 3-4, 2005.
[16] Wenyu Qu, Hong Shen, and John Sum, "New Analysis on Mobile Agents Based", Network Routing. *Applied Soft Computing Journal* (ASOC), Vol. 6, No. 1, Elsevier, 2005, p. 108-118.
[17] Stanley P. Y. Fung, Francis Y. L. Chin, Hong Shen, "Online scheduling of unit jobs with bounded importance ratio", *International Journal of Foundations of Computer Science*, Vol. 16, No. 3, 2005, p. 581-598.
[18] Qiangfeng Zhang, Francis Y. L. Chin, Hong Shen, "Minimum Parent-Offspring Recombination Haplotype Inference in Pedigrees", *Transactions on Computational Systems Biology*, Vol. 2, 2005, p. 100-112.

B. Book Chapters/Conference Proceeding Papers

[1] Hong Shen, "Flexible Mining of Association Rules", book chapter in *Encyclopedia of Data Warehousing and Mining*, IDEA Pub., USA, 2005.
[2] Hong Shen and S. Horiguchi, "Mining Quantitative and Fuzzy Association Rules", book chapter in *Encyclopedia of Data Warehousing and Mining*, IDEA Pub., USA, 2005.
[3] Keqiu Li, Hong Shen, Francis Y. L. Chin: Cooperative Determination on Cache Replacement Candidates for Transcoding Proxy Caching, *Lecture Notes in Computer Science* 3619 (Proc. of ICCNMC 2005), 2005, p. 178-187. (Best paper award.)
[4] Keqiu Li, H. Shen, Francis Y. L Chin, and Liusheng Huang. Multimedia Object Placement Solutions for Hybrid Transparent Data Replication. The IEEE Global Telecommunications Conference (GLOBECOM 2005), St. Louis, USA, November, 2005.
[5] Hui Tian and Hong Shen, "Discover multicast network internal characteristics based on hamming distance", *Proc. of 2005 IEEE International Conference on Communications* (ICC'05,), Seoul, Korea, May 2005, CD-ROM, IEEE Press.
[6] Hui Tian and Hong Shen, "An optimal coverage scheme for wireless sensor network", *Proc. of 2005 IEEE International Conference on Networks* (ICN'05), Reunion Island, France, April 2005, pp. 722-730, Springer-Verlag.
[7] Hui Tian and Hong Shen, "Hamming distance and hop count based classification for multicast network topology inference", *Proc. of The IEEE 19th International Conf. on Advanced Information Networking and Applications* (AINA'05), Taiwan, March 2005, pp. 267-272, IEEE press.
[8] Zonghua Zhang and Hong Shen, Constructing Multi-Layer Boundary to Defend Against Intrusive Anomalies: An Autonomic Detection Coordinator, *Proc. The Int'l Conf. on Dependable Systems and Networks* (DSN2005), Yokohama, Japan, June 2005.
[9] Z. Zhang, H. Shen, "Dynamic Combination of Multiple Host-based Anomaly Detectors with Broader Detection Coverage and Less False Alerts", *Proc. of IEEE Int'l Conf. on Networking* (ICN'05), P989-996, April 17-21, 2005, Reunion Island, France.
[10] Yawen Chen and Hong Shen, "An Improved Scheme of Wavelength Assignment for Parallel FFT Communication Pattern on a Class of Regular Optical Networks", *Lecture Notes in Computer Science* 3779 (Proc. of 2005 IFIP Int. Conf. on Networks and Parallel Computing), Beijing, Dec. 2005, Springer-Verlag, p.189-196.
[11] Wenyu Qu and Hong Shen. Theoretical Analysis on A Traffic-Based Routing Algorithm of Mobile Agents. *Proceeding of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'05)*, France, p. 520-526, Sep. 2005.
[12] Keqiu Li, Keishi Tajima, and Hong Shen. Cache Replacement for Transcoding Proxy Caching. *Proc. of IEEE/WIC/ACM Int'l Conf. on Web Intellig. (WI'05)*, France, p. 500-507, Sep. 2005.
[13] Haibo Zhang, Hong Shen, Haibin Kan, "Reliability-Latency Tradeoffs for Data Gathering in Random-Access Wireless Sensor Networks", *Lecture Notes in Computer Science* 3619 (Proc. GCC 2005), 2005, p. 701-712.
[14] Wenyu Qu, Hong Shen, Yingwei Jin, "Distribution of Mobile Agents in Vulnerable Networks", *Lecture Notes in Computer Science* 3619 (Proc. GCC 2005), 2005, p. 894-905.
[15] W. Chan, F. Y. L. Chin, Y. Zhang, H. Zhu, H. Shen, P. W. H. Wong, "Off-Line Algorithms for Minimizing Total Flow Time in Broadcast Scheduling", *Lecture Notes in Computer Science* 3595 (Proc. COCOON 2005), 2005, 318-328.
[16] Keqiu Li, Hong Shen, Francis Y. L. Chin, "Placement Solutions for Multiple Versions of A Multimedia Object", Proc. 8th *IEEE Int. Symp. on Object-Oriented Real-Time Distributed Computing* (ISORC2005), Seattle, USA, May 2005, p. 224-231.
[17] Yingpeng Sang, Hong Shen, Zonghua Zhang, "An Efficient Protocol for the Problem of Secure Two-party Vector Dominance", Sixth *Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies* (PDCAT 2005), 5-8 December 2005, Dalian, p. 488-492.

Award:

Best paper award by Chinese Computer Federation and IEEE Computer Society for paper "Cooperative Determination on Cache Replacement Candidates for Transcoding Proxy Caching" at International Conference on Computer Network and Mobile Computing (ICCNMC 2005).

助教授
宮地　充子
MIYAJI, Atsuko
http://grampus.jaist.ac.jp:8080/miyaji-lab/index-jp.html

研究グループ
電子社会のための安心基盤技術

専門分野
情報セキュリティ、数論アルゴリズム

拠点形成における研究テーマ
電子社会のためのセキュリティ検証

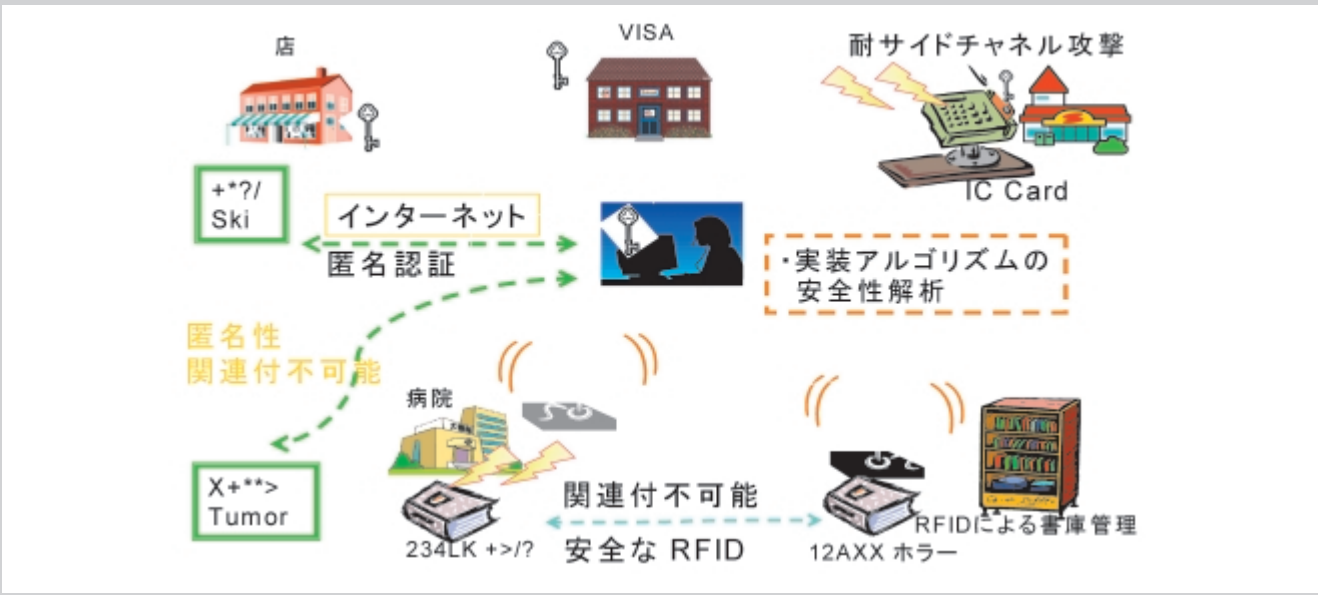
研究の目指すもの

安心性検証の統合システムの構築

携帯電話に代表される簡易な情報機器の爆発的な普及に伴い、社会システムの電子化が新たな展開期を迎えつつある。つまり、これまで人を介してなされていた諸サービスに代わり、インターネットと情報機器を介してなされる電子サービスが急速に普及しつつある。電子サービスの普及はこれまでの人を介したサービスには存在しない新たな問題を生み出すようになった。すなわち、第三者への個人データの流出、個人データの改ざんなどの問題である。

このような問題を回避するには、データの秘匿性・完全性の確保という情報セキュリティの研究が不可欠である。特に、容易性・便宜性を失うことなく、安全性を強化することは安心性検証のための重要な課題である。この安心性検証のための情報セキュリティ技術の３つの柱が、高速なデータ処理の秘匿性に必須の技術である共通鍵暗号、本人認証、データの完全性を実現するディジタル署名の必須の技術である公開鍵暗号の一種である（超）楕円曲線暗号、そしてこれら基盤技術を利用して実現するセキュアな電子プロトコルである。本研究開発では、これら３つの研究分野において最も近年重要視されている以下の問題の解決を目標とした。

1. 共通鍵暗号の安全性は絶対的な評価方法がなく、攻撃法に対する安全性を試行錯誤的に評価することが最大の問題である。本研究開発においては、共通鍵暗号の安全性にターゲットを絞り、統計的解析により安全性を解析する新しい理論の構築を目的とする。
2. 楕円曲線暗号は高速コンパクトな特徴からICカードで脚光を浴びている。ICカードでの利用は、電力消費量情報を利用するサイドチャネル攻撃への安全性が必須条件である。サイドチャネル攻撃は厳密なモデル化がなく、次々と新しい攻撃が提案され、その度、新しい安全策が必要になるという繰り返しが続いている。本研究はサイドチャネル攻撃のモデル化と安全性の証明をすることを目的とする。
3. 複数システム統合時の問題はユーザのプライバシ情報が結合することにより、必要以上のプライバシが漏洩することである。本研究開発では、システム統合時のユーザのプライバシ漏洩を防ぐ、公開鍵暗号システムの実現を目的とする。



以上の研究により信頼性の一段と強化された共通鍵暗号、楕円曲線暗号、プライバシ強化されたシステム統合の提供が可能になり、電子サービスの普及における効果は計り知れない。

拠点形成に関連する最近の研究テーマと成果

1. 共通鍵暗号の理論的安全性評価手法の確立

共通鍵暗号 RC 6 の解読アルゴリズムを改良し、計算量・メモリ量を削減した攻撃アルゴリズムを提案。
この結果、未解決問題であった 16 段以上の RC6 の解読が可能であることを理論的に証明した。

2. サイドチャネル攻撃に対する対策

－超楕円曲線暗号のサイドチャネル攻撃に安全かつ効率的なアルゴリズムを提案。これにより、既存法より効率的かつ安全性な超楕円曲線暗号を実現した。

－既存方法は安全性、計算効率が固定されて、任意のシステムに不向きである。本研究ではサイドチャネル攻撃への安全性と計算効率をフレキシブルに設定可能な方式を提案した。本方式により、安全性と効率がフレキシブルに設定可能なシステムの提供を実現した。

3. 複数システム統合時の安全性実現

ユーザの ID を公開鍵とする ID ベース暗号の新概念として、ユーザの ID が階層構造を持つ場合の暗号方式を構築した。これにより、ディジタル放送において、著作権保護を実現しつつ、複数のプロバイダによるコンテンツ配信時においても、ユーザのプライバシを確保しつつ、効率的なデータ配信が実現可能にした。

拠点形成に関連する主な業績

International conference （査読付のみ）

[1] A. Waseda, M. Soshi, and A. Miyaji. "n-state quantum coin flipping protocol", A International Conference on Information Technology - ITCC2005, Volume II, pp.776-777, 2005
[2] A. Miyaji and Y. Takano. "On the Success Probability of chi^2-attack on RC6", Proceedings of ACISP 2005, Lecture Notes in Computer Science, 3089(2005), Springer-Verlag, 310-325.
[3] H. Mamiya and A. Miyaji. "Fixed-Hamming-Weight Representation for Indistinguishable Addition Formulae", ACNS 2005.

論文

[1] A. Waseda, M. Soshi, and A. Miyaji."Quantum coin flipping protocol using n-dimensional quantum states", IPSJ Trans., vol. 46, No.8(2005), 1903-1911.
[2] A. Miyaji and K. Umeda."Efficient Group Signature Scheme based on a Modified Nyberg-Rueppel Signature", IPSJ Trans., vol. 46, No.8(2005), 2107-2119.
[3] A. Miyaji and Y. Sakabe and M. Soshi."Java Obfuscation -- Approaches to Construct Tamper-Resistant Object-Oriented Programs", IPSJ Trans., vol. 46, No.8(2005), 2107-2119.

招待講演

[1] A.Miyaji. “Privacy Rights in the Digital Age Technological, -How to Protect Privacy Right by the technology of Information Security-”, International Forum on Privacy Rights in the Digital Age, Korean National Commission for UNESCO, September 2005.
[2] 宮地 充子（招待講演）「ユビキタス社会と情報セキュリティ」，サイバネティック・フレキシブル・オートメーション (CFA) 研究分科会第 20 回研究例会 , 2005.
[3] 宮地 充子 , 近澤 武 , 竜田 敏男 , 大塚 玲 , 安田 幹 ,（解説）「情報セキュリティの標準化動向について－ ISO/IEC JTC1/SC27/WG2 2005 年 4 月ウィーン会議報告－」，電子情報通信学会，信学技報 ISEC 2005-30(2005), 155 - 164.
[4] 宮地 充子「双線形写像に基づく暗号に適した（超）楕円曲線の構成」,「代数幾何・数論及び符号・暗号」研究集会報告書，東京大学大学院数理科学研究科，(2006), Jan

新聞掲載

・「ニューズウィーク日本版」（2005・10・26 号）「世界が尊敬する日本人 100 人」
・「週刊文春 BUSINESS」（2006・4・5 号）「40 代・日本のキーマン 300 人」

特任助教授
双紙　正和
SOSHI, Masakazu
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00073soj.html

研究グループ
電子社会のための安心基盤技術

専門分野
情報システムセキュリティ理論、
セキュリティシステム評価検証

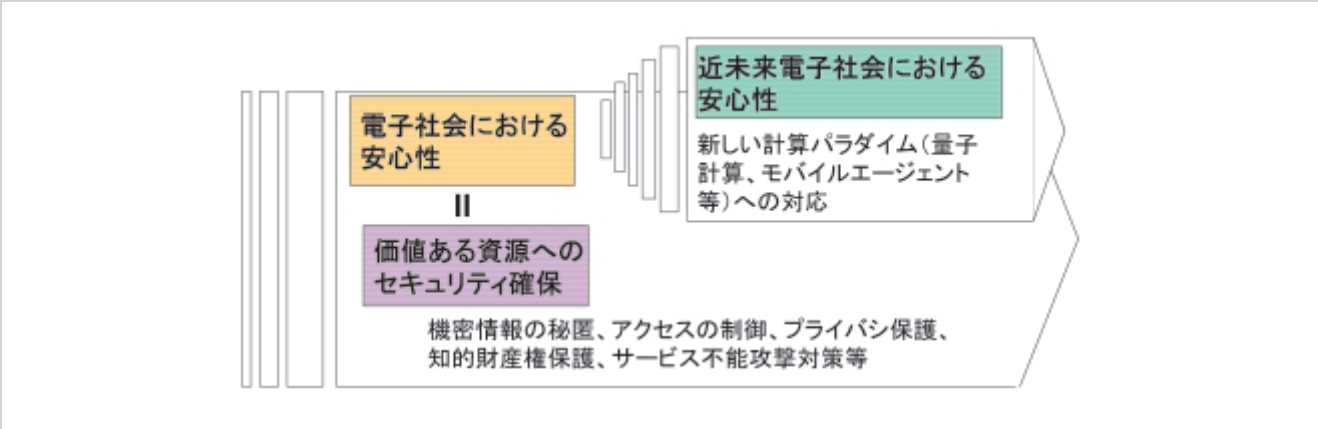
拠点形成における研究テーマ
電子社会のためのセキュリティ検証

研究の目指すもの

電子社会においては、行政や企業などにおける様々な情報がディジタルデータとして流通する。ディジタルデータは、改変や複製が容易であるという特徴を持っている。このため、ディジタルデータとして実現される機密情報の秘匿、アクセスの制御、プライバシ保護、知的財産権保護、サービス不能攻撃対策など、情報セキュリティの確立が、電子社会の安心性要件として必須である。これらは、一言で言えば、電子社会における、価値ある資源（情報を含む）に対するセキュリティ確保ということができる。また、近年、新たな計算パラダイム（量子計算、モバイルエージェント等）が出現し、電子社会を取り巻く環境は急激に変化しつつある。電子社会における安心性を確保・検証するためには、こういった状況を考慮に入れる必要がある（図 1）。そこで、本研究は、以下の２点の観点から、電子社会における安心性を検証する方法を開発することを目標とする。

1. 電子社会における安心性…アクセス制御、プライバシ保護、知的財産権保護、サービス不能攻撃対策
2. 近未来電子社会における安心性…量子セキュリティプロトコル、モバイルエージェントセキュリティ

図 1. 電子社会における安心性要件の概念



拠点形成に関連する最近の研究テーマと成果

（1）耐タンパーソフトウェアに関する研究

近年、Java、JavaScript、スクリプト言語等、ソースコードもしくはそれに近い形式でのソフトウェア配布が増えてきている。そのような状況では、ソフトウェアの機密データや重要アルゴリズムが盗用される危険性が生じる。そのため、知的財産権の保護の為には耐タンパーソフトウェアが必要となる。特に、耐タンパー化を実現するための手段として、難読化が注目を浴びている。

しかしながら、従来のソフトウェア難読化技術は理論的な根拠を持っておらず、その効果について疑問が残るものが多かった。そこで、プログラムにおける関数間の解析が困難であることに着目し、それに基づいた難読化手法を提案した。また、オブジェクト指向言語の特徴を利用した難読化手法について研究を行った（参考文献 1）。それらは、難読化されたプログラムの解析の困難さに、一定の理論的根拠を与えることができるという特徴を持っている。また、難読化ツールの実装を行い、評価を行っている。

耐タンパーソフトウェア、難読化とは

耐タンパーソフトウェアとは、ソフトウェアに対する不正なリバースエンジニアリング（解析、改変）を困難としたソフトウェアである。難読化は耐タンパーソフトウェアを実現する方法の一つであり、そのままの形で実行はできるが、プログラムの解析を困難なものに変換する技術である。

(2) サービス不能攻撃対策の研究

近年、攻撃者が大量のパケットを標的サーバに送信し、そのサーバをダウンさせてしまう、サービス不能攻撃が、電子社会における大きな脅威となっている。一般的にいって、サービス不能攻撃の対策は非常に困難であり、有効な対策を考えることが、電子社会における安心性確立のためには必須である。ここで、サービス不能攻撃対策は、以下の２種類に大きく分類できる：(1)攻撃発生時におけるネットワークの輻輳を緩和させる方式、および、(2)攻撃者の位置を特定できることにより、攻撃を未然に防ごうとする方式。本研究では、(1)に関して、ルータの協調によって、攻撃パケットを効率的にフィルタリングする方式、(2)に関しては、ルータごとに異なる確率でパケットにマーキングを行い、それらの情報によって、従来手法より効率よく攻撃者を特定可能な方式について提案を行い、評価・検証した。

(3) 量子セキュリティプロトコル…量子複数秘密分散の研究

現在、コンピュータの性能は飛躍的に向上しており、チップの集積度、発熱量、性能等に関して限界に近づきつつある。これらの問題点を解決するものとして、量子力学的原理に基づく量子計算(機) やそのプロトコルが注目を浴びている。中でも、量子通信は既に実用化段階に達しつつある。そこで、近未来における電子社会の安心性に対して、このような量子計算がどのような影響を及ぼすかを検証することは極めて重要である。本研究では、量子コイン投げプロトコル、量子秘密分散法等をまず対象として、量子計算・プロトコルを確立、評価・検証する。

今までの成果

1. *n*状態量子コイン投げプロトコル

*n*次元量子状態を使用する量子コイン投げプロトコルを提案した。一方のユーザの不正成功確率を犠牲にすることで、もう一方のユーザの不正成功確率を任意に小さくすることができる。これは、従来の量子コイン投げプロトコルの一般化である（図２、参考文献２)。

2. 量子複数秘密分散法

複数の秘密量子状態をもつことができる、量子秘密分散法を初めて提案した（図３、参考文献３)。

基本的な概念

- **コイン投げプロトコル**
  二人のユーザ（不正を行うことを想定）が、公正に１ビットの値について合意する手法。さまざまなセキュリティプロトコルにおける重要な要素技術である。
- **秘密分散法**
  秘密情報を、複数の分散情報（シェア）に符号化し、秘密を復元可能なユーザの集合（有資格集合）のシェアを集めると、その秘密を復元することができるが、有資格集合とはならないユーザの集合に対しては一切の秘密を漏らさないような符号化法。
- **量子状態** $|\psi\rangle$
  内積を定義できる複素ベクトル空間の単位ベクトルとみなすことができる。

図２. *n*状態量子コイン投げプロトコル（*n*＝３の場合）

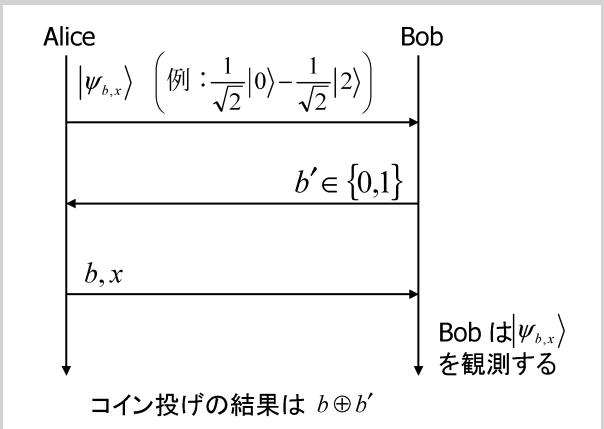
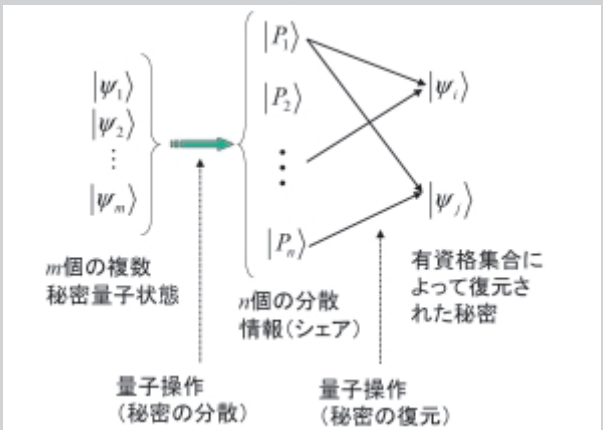


図３. 量子複数秘密分散法



拠点形成に関連する主な業績

[1] Yusuke Sakabe, Masakazu Soshi, and Atsuko Miyaji, Java obfuscation - approaches to construct tamper-resistant object-oriented programs, IPSJ Journal, Vol. 46, No. 8, pp. 2107-2119, 2005.
[2] 早稲田篤志，双紙正和，宮地充子，n次元量子状態を使用した量子コイン投げプロトコル，情報処理学会論文誌，46巻，8号，pp.1903-1911, 2005.
[3] 早稲田篤志，双紙正和，宮地充子, MSPを使った量子複数秘密分散に関する考察, IEICE Japan Tech. Rep., ISEC2005-119, pp.53-60, Dec. 2005.

情報科学研究科

教授
日比野　靖
HIBINO, Yasushi
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00042soj.html

研究グループ
電子社会のための安心基盤技術

専門分野
計算機アーキテクチャ

拠点形成における研究テーマ
安心電子社会のためのハードウェア・キーコンポーネントの研究

研究の目指すもの

安心な電子社会の実現には、その基盤となるハードウェアに対して高い信頼性が求められるだけでなく、システムに対する攻撃や、システムの誤操作に対して安全であることが求められる。システムの安全を保つためには、システムの基盤を構成するハードウェアのキーコンポーネントに、安全を保証する機構が備わっていなければならない。すなわち、ここだけは絶対に破壊されず信頼できるという中核部分が必要である。

本研究では、このようなハードウェアキーコンポーネントを明らかにして、その構成法を確立し、また実装まで含めた実現法を追究する。

拠点形成に関連する最近の研究テーマと成果

（1）ハードウェア化に適した新しい公開鍵暗号方式の提案

公開鍵暗号では、受信者が復号化の秘密鍵 s を持ち、送信者は公開された鍵 k により暗号化を行う。ElGamal タイプの公開鍵暗号の解読の困難性は、離散対数問題の困難性を利用したものであり、安全性の確保のためには、元の数が大きな体 F_p が用いられる。

Lenstra は、整数 q の体 F_q の 6 次の拡大体 F_q^6 の元が、そのトレースをとることにより、2 次の拡大体 F_q^2 の元で表現できることを利用した、新しい公開鍵暗号方式 XTR（Efficient and Compact Subgroup of Trace Representation）を提案している。XTR では、鍵の長さ、暗号文の長さを、安全性を同一に保ちながら、従来の公開鍵暗号の 1/3 に短縮できる。

本研究では、整数 q として、3 の奇数巾 ($q=3^{2k+1}$) を用いること、すなわち標数 3 の体を用いることにより、体 F_q の 6 次の拡大体 F_q^6 の元が、そのトレースをとることにより、もとの体 F_q の元で表現できることを見いだし、トレースの計算をするアルゴリズムを具体的に与えた。

この標数 3 の体を用いる XTR では、Lenstra のオリジナルの XTR より、鍵の長さ、暗号文の長さをさらに 1/2 に短縮できる。さらに、標数 3 の体の実装に、三値論理を用いることにより、効率のよいハードウェア実装が可能なことを示し、その性能を評価したところ、これまでのソフトウェア実装に比べ約 100 倍の高性能化が図れることを示した。

図 1. 標数 3 の体を用いた XTR による暗号化・複合化

```
Plain text:      abcdefghijklmnopqrstuv
Encrypted code: 00112222001012100110112202200120111121122012021020010210
                22211001100101201110221102012100222001122012200100102l0

Decryptedcode:  02102021100211102112021200212102122022000220102202022100
                22110221202220022210222210000100011000210010100111001201
Decrypted text: abcdefghijklmnopqrstuv
```

(2) 三値論理回路の構成法と暗号ハードウェアへの応用

これまで、三値論理回路として、二値のCMOS論理回路のように、高速でかつ定常時には電流が流れないことによる低消費電力性を備えたものは無かった。

これに対してOlsonは、CMOS回路で定常時に電流が流れない三値論理回路の構成法を示したが、すべての三値論理関数を実現するには回路構成が複雑になるという問題があった。

本研究では、MOSトランジスタの特徴を生かしたトランスファーゲート論理を用いることにより、一変数の三値論理回路（Olson法により実現）と、CMOSトランスファーゲート論理による選択回路とを組み合わせる方法（TG法とよぶことにする）により、スイッチング特性が良好な二変数三値論理関数回路を組織的に実現する方法を与えた。（特許出願２件）

TG法による回路実現法と、また三値の表現として対称三値を用いることにより１桁の乗算の結果が１桁になる性質を生かして、さまざまな暗号ハードウェアで必須となる高速の大規模乗算器をコンパクトに構成できること示した。 特に、三値論理を用いることで、部分積加算部を4-2レデューサーで構成できることから、配線の交差数を二値を用いる場合に比べて約１桁少なくできるので、面積の大幅な削減が可能となり、二値の場合の二倍の規模の大規模乗算器が同一面積で実現可能なことを示した。

図２. TG法による二変数三値論理関数の実現法

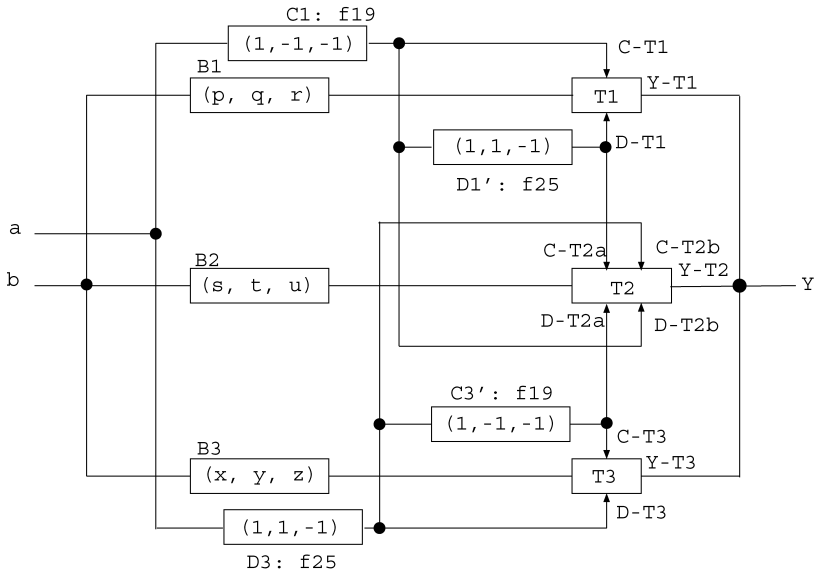
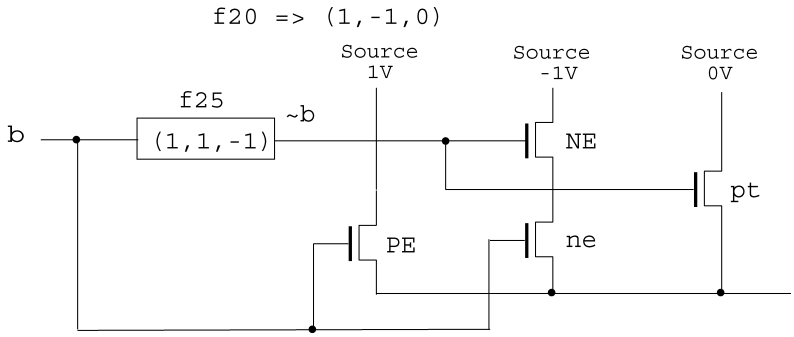


図３. 一変数対称三値論理回路の例



拠点形成に関連する主な業績

[1] Masaaki Sirase, Yaushi Hibino, An architecture for Elliptic Curve Cryptograph Computation, ACM SIGARCH Computer Architecture News, Vol.33, Issue 1 (mar 2005) Workshop on Architectural Support for Security and Ant-Virus (WASSA), pp.124-133 (Oct 2004)
[2] 白勢 政明, 日比野 靖, CMOSトランスファーゲートによる三値論理回路とその構成法, 多値技法, Vol.MLV-05, No.1, pp.80-89 (2005.1)
[3] 白勢 政明, 日比野 靖, 標数３の体でのXTR, 信学技法, Vol.105, No.51, (ISEC2005-3), (2005.5)
[4] 白勢 政明, 日比野 靖, XTRに適したディジタル署名方式, 信学技法, Vol.105, No.395, (ISEC2005-96), (2005.11)
[5] 日比野 靖, 白勢 政明, 三値論理関数回路および多論理関数回路, 特願2005-001866 (2005.1)
[6] 日比野 靖, 白勢 政明, 三値論理関数回路, 特願2006-023474 (2006.1)

情報科学研究科

教授
金子　峰雄
KANEKO, Mineo
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00050soj.html

研究グループ
電子社会のための安心基盤技術

専門分野
集積回路理論、設計、最適化

拠点形成における研究テーマ
電子社会の高信頼アーキテクチャ

研究の目指すもの

集積回路は、人間の活動をサポートし、豊かで安全・安心な社会・生活環境を実現する情報化、インテリジェント化の根本デバイスであって、集積回路、集積システムの高信頼化は安心電子社会基盤をまさに基盤から支える重要な技術です。集積回路は、数ミリから十数ミリ角の基盤の上に極微細なパターンを刻んで膨大な数のトランジスタとそれらの間の接続を作り込んだ電子回路であり、そこを流れる電気信号によって「計算」を実行するものです。こうした集積回路を高性能かつ高信頼に働かせるための諸技術の開発を行い、安心電子社会の基盤をつくることを目標としています。

集積回路には設計、製造、稼動の側面があり、（1）設計の不完全性、（2）製造時の欠陥混入、（3）動作時の非理想性（外乱、経年変化など）のそれぞれに対して高信頼化、信頼性保証を行う必要があります。特に本研究では、これら（1）、（2）、（3）に対して集積回路システム設計の立場からの解決を目指しています。

現在および将来の具体的検討課題は以下の通りです。

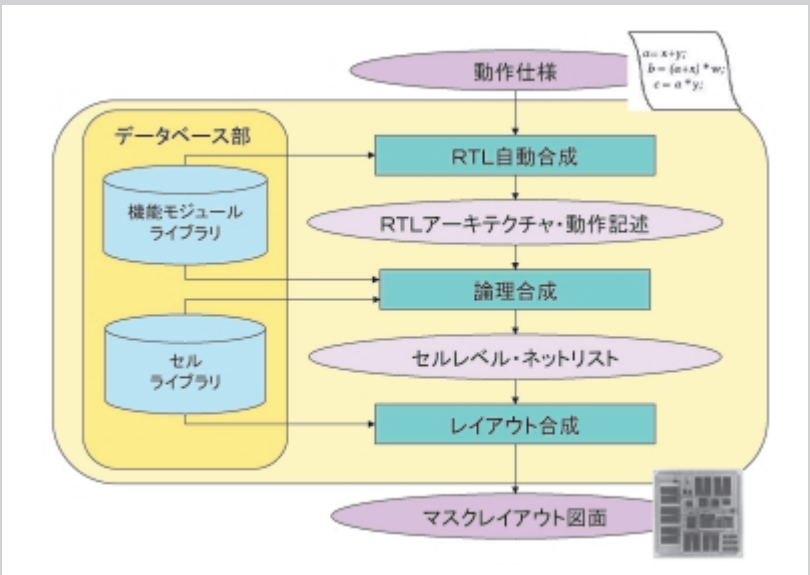
- ▶ 設計の高信頼化：設計仕様から集積回路の最終的設計図であるレイアウト図までの各設計段階で、人手を完全に排除し、設計を完全自動化する技術、設計の諸段階で正しさを保証して記述変換する技術、設計仕様そのものの正しさを保証する技術、など。
- ▶ 製品の高信頼化：大規模集積回路システムに対するテスト技術、テスト容易化のための回路設計技術、　製造時の欠陥混入を低く抑えるレイアウト設計技術、欠陥を含んでいても所望の回路ネットワークを再現できる冗長化と再構成の技術、など。
- ▶ 動作の高信頼化：ノイズ耐性を有する回路・アーキテクチャ技術、論理誤りに対する誤り検出と誤り訂正、特にリアルタイム性に配慮した誤りマスキング・誤り訂正の技術、遅延変動に対する耐性を有する回路・アーキテクチャ技術、長時間連続動作のための低消費電力回路・アーキテクチャ技術、など。

拠点形成に関連する最近の研究テーマと成果

（1）集積回路システムのレジスタ転送レベル自動合成

集積回路システムの設計自動化は、集積回路システムを設計する際に人手介入を極力排除して人為的誤りを回避し、高性能、高信頼な設計を行おうとするものです。この中で「レジスタ転送レベル（RTL）合成」は、実現すべき計算アルゴリズム記述（仕様）からレジスタ、演算モジュールレベルの回路構造記述と制御記述を自動生成するシステムであり、以降に続く論理合成、レイアウト合成と組み合わされて、設計仕様からの集積回路自動合成を実現するものです。

図 1. 動作仕様から集積回路のマスク図面を生成する自動合成の全体像



（A） クロックレス・データパスの制御スキュー最適化とRTL 合成：
同期システムが本質的に有する大きな問題として、クロック信号をシステム全域に供給するための資源的、消費電力的オーバーヘッドがあります。データ処理部からクロック信号を排除したクロックレス・データパスにより、こうしたオーバーヘッドを大幅に縮小します。

- ▶ 計算アルゴリズム（動作仕様）から RTL 合成の自動化による高信頼設計
- ▶ クロックレス・データパス・アーキテクチャの提案・採用による低消費電力化
- ▶ 制御スキュー（モジュール動作のタイミング調整）による高性能化（動作速度の向上、ピーク電力の抑圧）[1]

（B） 自己同期データパスの同期モデルと RTL 合成：
クロック信号に伴う諸問題を解決するもう一つの考え方として、クロック信号を完全に排除して、その代わりに信号到着を自己認識しながら計算ステップを自ら進めていく自己同期（あるいは非同期）アーキテクチャがあります。高性能な自己同期データパスを自動合成するシステムを研究、開発しています [2][3]。

- ▶ 稼動時の信号伝播遅延の変動に対する高い耐性を有する自己同期アーキテクチャ
- ▶ 計算アルゴリズム（動作仕様）から RTL 合成の自動化による高信頼設計
- ▶ 新しいレジスタ構成による高いレジスタ共有性
- ▶ 資源割当優先の解空間探索による高品質な RTL 合成解生成

（2） 実時間誤り訂正アーキテクチャと合成

集積システム稼動時の外乱等による一時的計算誤りや経年変化等による故障に対して、正しい計算結果を出し続けるためのメカニズムと、それを含めた集積システムの最適化、設計自動化について検討を行っています。

（A） 計算アルゴリズムの冗長化と多数決書き戻し方式
アプリケーション専用アーキテクチャを対象に、単一故障による計算誤りを訂正可能な「多数決書き戻し方式」を提案し、誤り訂正を保証する条件、自動合成を開発しています。

- ▶ 計算モジュール、レジスタ、結線、多数決器の全てを故障対象として、任意の単一故障に対して正しい計算結果を保証。
- ▶ 計算アルゴリズム（仕様）から、冗長計算の自動挿入、自動 RTL 合成による高信頼設計

図 2. レジスタ間信号遅延に基づくタイミング図：完全同期設計（上）と制御スキューの導入による高速化（下）の様子

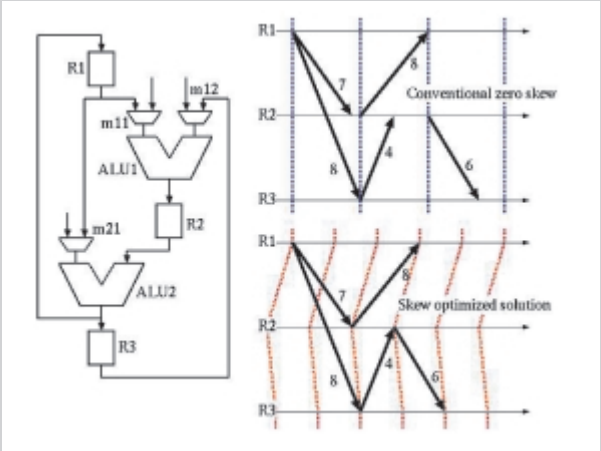


図 3. 自己同期システムではデータの到着がトリガーとなって、計算のステップが進んで行く。

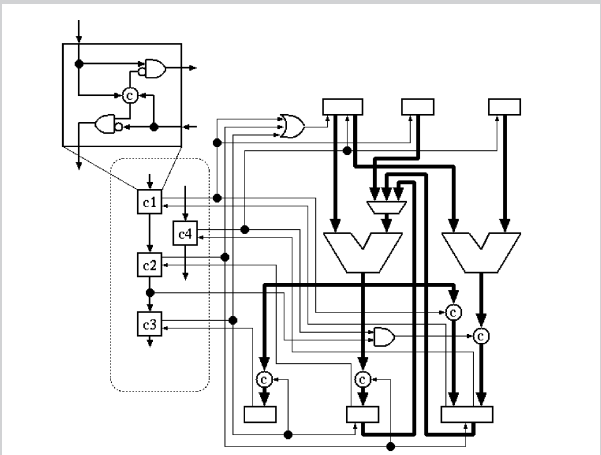
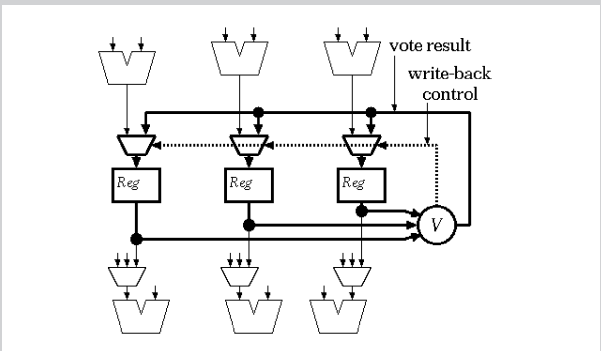


図 4. 計算アルゴリズムの多重化とレジスタへの書き戻し方式にて、実時間誤り訂正可能システムを構成する。



拠点形成に関連する主な業績

主要論文

[1] Takayuki Obata, Mineo Kaneko, “Control Signal Skew Scheduling in RT Level Datapath Synthesis,” Proc. of IEEE International Midwest Symposium on Circuits and Systems, ISBN:0-7803-9198-5 (2005)
[2] Koji Ohashi, Mineo Kaneko, “Statistical Analysis Driven Synthesis of Asynchronous Systems,” Proc. of International Conference on Computer Design, pp.200-205 (2005)
[3] Koji Ohashi, Mineo Kaneko, “Statistical Scheduling Length Analysis in Asynchronous Datapath Synthesis,” Proc. of IEEE International Symposium on Circuits and Systems, pp.700-703 (2005)

情報科学研究科

教授
浅野　哲夫
ASANO, Tetsuo
http://www.jaist.ac.jp/~kkgi/thisyear/soj/00033soj.html

研究グループ
電子社会のための安心基盤技術

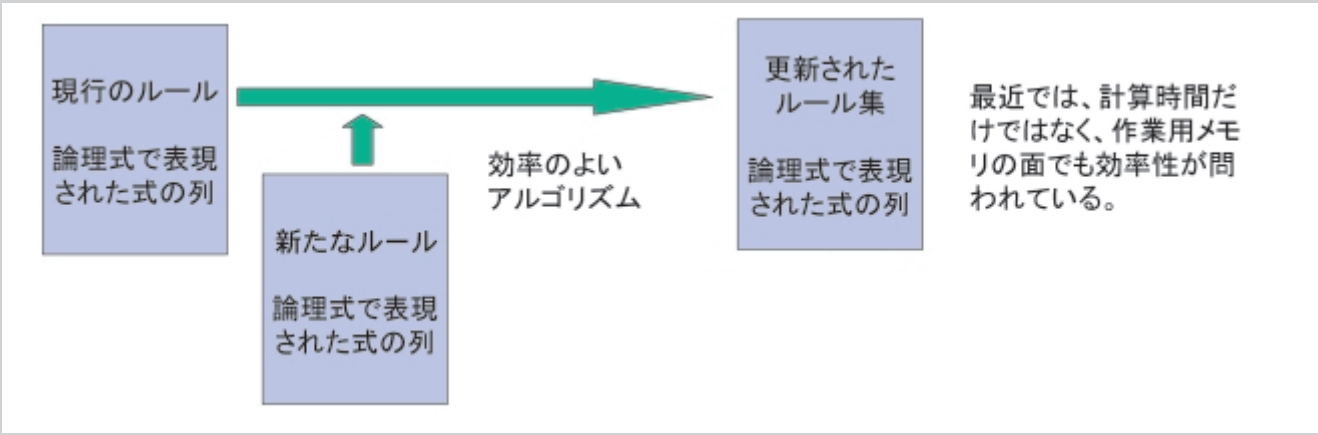
専門分野
アルゴリズムと計算幾何学

拠点形成における研究テーマ
アルゴリズムの効率化に関する研究

研究の目指すもの

安心電子社会基盤を構築するにあたって、様々な側面でプログラムの効率化が求められる。プログラムの高速化はどんな状況においても必要であるが、単に高速化を達成すればよいというものではなく、実はもっと本質的な意味をもっている。計算複雑度の研究分野では、計算機によって解ける問題を、妥当な時間内に解ける問題と、妥当な時間内に解くことが絶望的な問題（扱いにくい問題）に分類している。数学的には、入力のサイズの多項式時間で解けるのが前者の問題で、指数時間以上かかることが予想される問題が後者の難しい問題である。ここで「予想される」と書いたのは、有名な「P ≠ NP」予想が未だに証明されていないからである。

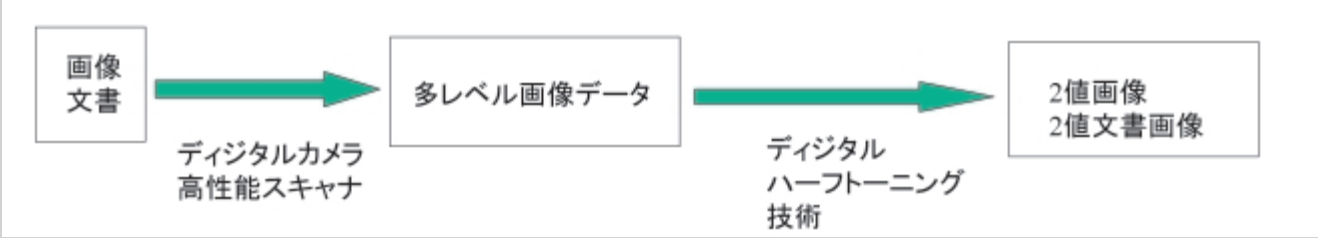
本研究グループでは、アルゴリズムの実行に必要な計算時間を推定する方法を確立するとともに、時間によって変化しない定性的な部分に対して適切な前処理を施しておくことによって動的な変化に迅速に対応するための方法論を構築することを目指す。



拠点形成に関連する最近の研究テーマと成果

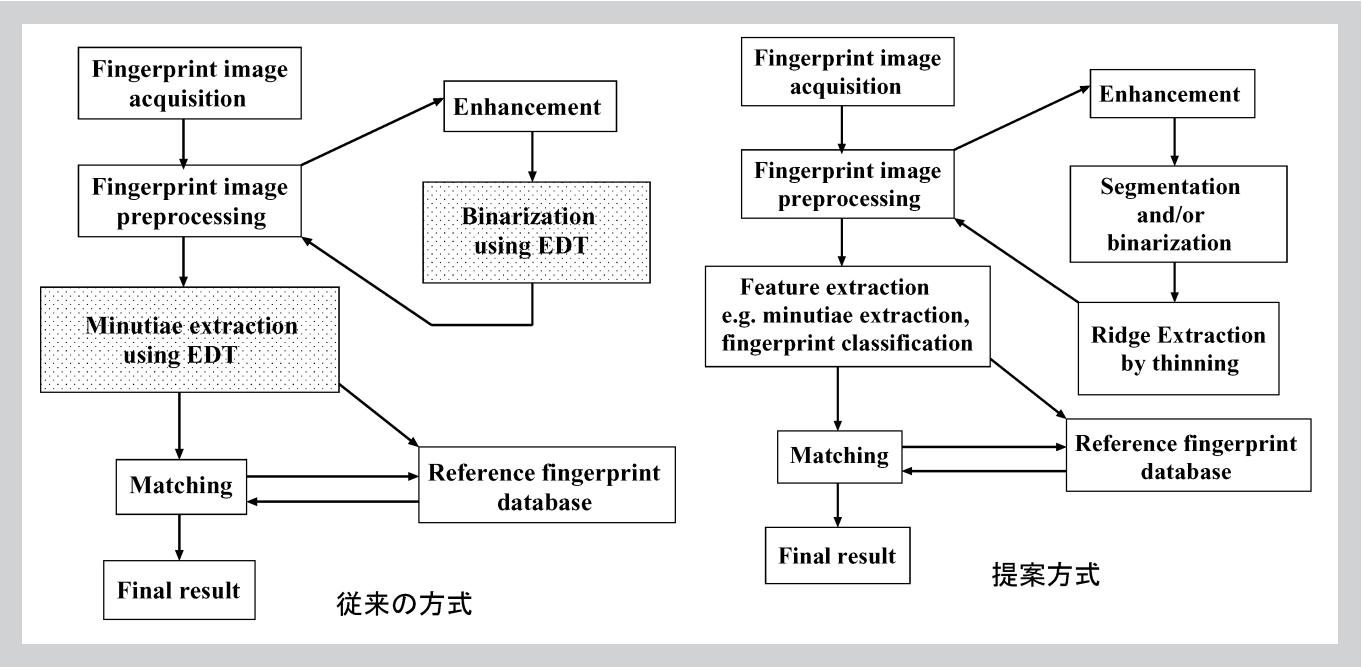
組み合わせ最適化に関する研究

ディジタルカメラなどで取り込まれた多レベルの画像を印刷用に２レベルの画像に変換する技術であるディジタルハーフトーニングは安心電子社会にとっても重要な研究テーマである。最近になって、公式文書を電子的に蓄えることが可能になった。そのために、スキャナーなどで取り込まれた文書画像を２値画像に変換する技術は重要さを増している。本研究では、２値化の問題を組み合わせ最適化の問題として定式化し、その計算複雑度を解析するとともに、ほぼ最適な２値化を達成する近似アルゴリズムの設計も行っている。これらの結果は世界的にも注目を集め、2005 年には２つの国際会議で招待講演を行っている。



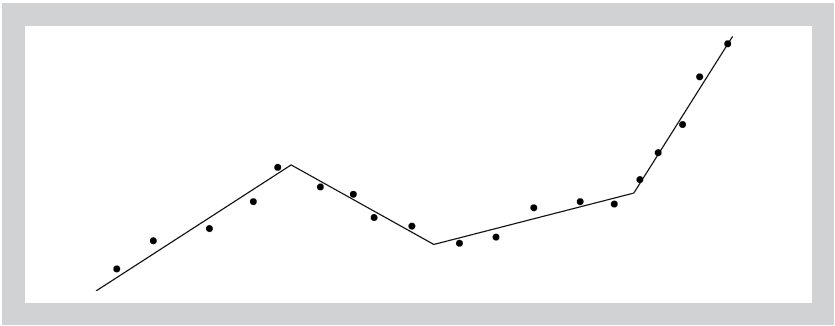
指紋同定・認識に関する研究

安心電子社会を実現するためには、個人の同定・認識が重要である。現在最もよく使われているのが指紋である。入出国管理にも使われるなど、指紋同定は既に実用化のレベルにあるが、解決すべき問題点も数多く残っているのが現状である。本研究では、本 COE プログラムによって雇用されている博士後期課程の学生（LIANG Xuefeng）と共同で、指紋の入力から同定・認識までのシステム開発を行ってきた。特徴は、高速距離変換の技法を駆使することによって、入力の画質と認識率の向上を実現していることである。これらの研究成果は、複数の国際会議と論文誌に発表している。



計算幾何に関する研究

社会生活の様々な場面で幾何的な情報が含まれている。たとえば、工事現場の表示や、工事による迂回路の設定など、市民への適切なフィードバックを実現するためには幾何に関連する問題を解決する必要がある。幾何問題を解決するためには幾何情報を入力しなければならないが、現実の幾何データは任意曲線で定義されていることがあり、そのままでは計算が難しい。そこで、曲線上の点列を直線で近似するという作業がしばしば要請される。いわゆる直線当てはめの問題である。この問題は最小２乗法によって効率よく解けることが知られているが、与えられた点列を２本以上の線分の列として近似する問題はあまり考えられなかった。本研究では、さらに一般に与えられた点列を k>1 本の線分列で最適に近似する問題の計算複雑度について考察し、最適解を妥当な時間で求めることは難しいが、近似解であれば高速に求めることができることを示している。



拠点形成に関連する主な業績

[1] T. Asano, M. de Berg, O. Cheong, H. Everett, H. Haverkort, N. Katoh, and A. Wolff: "Optimal Spanners for Axis-Aligned Buildings," Computational Geometry: Theory and Applications，採録決定
[2] B. Aronov, T. Asano, Y. Kikuchi, S. C. Nandy, S. Sasahara, and Takeaki Uno: "A Generalization of Magic Squares with Applications to Digital Halftoning," to appear in Theory of Computing System.
[3] T. Asano, M. de Berg, O. Cheong, H. Everett, H. Haverkort, N. Katoh, and A. Wolff: "Optimal Spanners for Axis-Aligned Buildings," Computational Geometry: Theory and Applications, 30, 1, pp.59-77, January 2005.
[4] T. Asano, "Computational Geometric and Combinatorial Geometric Problems Related to Digital Halftoning," (Invited Talk) Computing: The Australasian Theory Symposium, 2006.

教授
赤木　正人
AKAGI, Masato
http://www.jaist.ac.jp/~akagi/

研究グループ
電子社会のための安心基盤技術

専門分野
音声信号処理

拠点形成における研究テーマ
安全なヒューマンーマシン・インターフェースの構築

研究の目指すもの

人間社会と電子社会のインターフェースが高度にしかも安全に構築されることは重要である。本研究では，特に音声による安全なヒューマンーマシン・インターフェースの構築を目指す。音声によるヒューマンーヒューマン・コミュニケーションでは、環境雑音とか残響などの様々な外乱がある状況で、「何を話しているのか」などの言語情報のみならず、「誰が」「どのような表情で」「どのような心理状態で」などの非言語情報をも送受している。安全なヒューマンーマシン・インターフェースを構築する場合、これらすべてを考慮した上で、システムの設計を行う必要がある。
ところで、音声によるヒューマンーヒューマン・コミュニケーションの中心である音声を聞く・話すは人間の固有の営みである。このため、音声における人間の営みを知り人間の営みを記述（モデル化）することで、高度な音声処理システムを構築することができると考えられる。本研究では、「聞く」「話す」のモデルを計算機上に構築することで、安全なヒューマンーマシン・インターフェースを実現することを目的とする。

拠点形成に関連する最近の研究テーマと成果

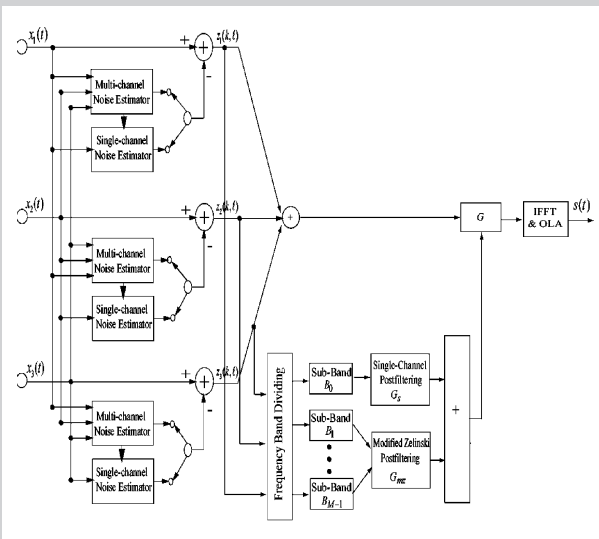
（1）「聞く」に関するモデル化とその応用

人間は、雑音環境中から目的の音を難なく選択して知覚することができる。この機能は人間を含む動物の聴覚に備わる有用な機能であり、カクテルパーティ効果と呼ばれる。カクテルパーティ効果は、（1）二つ以上の音源が同時に呈示されたとき着目する音源のみを選択的に聴取できること、（2）カクテルパーティのように多数の話者の音声が混在している状況の中で希望する話者の声を選択して聞くことができることからこの名前が付けられた。カクテルパーティ効果が生じる原因としては、それぞれの音源に対して両耳聴によって知覚される音像の空間的位置（方向と距離）の違い、音の大きさ、ピッチ、音色など音源の特性そのものの違い、また音声の場合には言語的知識、発話者の口の動きなどの視覚的情報、経験などが関係していると見られている。これらを手掛かりとするカクテルパーティ効果の機能をモデル化することができれば、音声認識、音声分離、雑音抑圧に有用なツールが構築できる。本研究では、苛酷な環境（雑音環境、残響環境）でも頑健な“聞く”システムの構築を目指して、次の二つの研究を遂行している。

（1-a）小規模マイクロホンアレイによる複数雑音除去

本研究では、自動認識システムの認識精度を改善すること目的とした雑音抑制システムを提案している。実環境に存在する雑音は色々な種類の音源から発せられ様々な特性をもつため、できるだけ雑音特性に依存しない抑圧システムが望ましい。ここでは、雑音を方向性雑音と非方向性（拡散性）雑音にわけ、方向性雑音に対してはマイクロホンアレイを用いたビームフォーミング、非方向性雑音に対してはウィーナー・フィルタを基礎としたポストフィルタリングを提案した。これらのビームフォーマとポストフィルタを組み合わせた結果、本システムは、ある方向からの雑音や拡散した雑音、また定常な雑音やそうではない雑音を含む様々な種類の雑音を扱うことができる。また、音声認識システムのための前処理システムとして本雑音抑制システムを検証したところ、本雑音抑制システムが、従来のアルゴリズムより音声認識パフォーマンスをより改善し優れることが示された。

図1　3チャンネルマイクロホンアレイ



（1-b）聴覚情景解析にもとづいた音源分離

我々の研究室では、目的音の波形を雑音成分から分離する方法についてすでに提案している。この手法では、雑音中に目的音が存在した場合分離は成功、存在しない場合は分離不可能となる。これを用いて、目的音が存在すると仮定した場合の分離可能性を検証することで音声認識を行う、新しい音声認識方式を提案した。

（2）「話す」に関するモデル化とその応用

音声に含まれる非言語情報の研究の一環として、我々は、個人性、感情、歌声などがどのように知覚されているのかについて興味を持ち、総合的に研究を行っている。その中で、特に歌声と感情音声について、（1）どのように歌声の質、たとえば「自然性」あるいは「歌声らしさ」、が知覚されているのか、（2）どのような物理特徴が話し手の感情を聞き手に生起させるのか、を取り組む問題として，次の二つの研究テーマを遂行している。

（2-a）歌声の合成

本研究では、話声（歌詞の朗読音声）に歌声特有の非言語情報を付加することで、より自然な、歌声らしい歌声の合成を試みる。「歌を歌う」ためには、（1）メロディ・リズムにあわせて音程を激しく変化させる、および、（2）自分自身の声色を保ちつつ歌詞を伝えることが必要である。歌声合成のために、Source-Filter モデルを採用するとすれば、(a)メロディ変化に合わせた基本周波数制御、(b)スペクトル変形に合わせたフィルタ制御、および、(c)リズムに合わせた音韻長制御が必要となる。本研究では、図３に示すモデルを用いて、歌声合成を行っている。合成音の品質は、人間が歌唱した歌声と遜色ないものとなっている。

（2-b）感情音声の知覚モデルの構築

本研究では、非言語情報として感情音声を取り上げ、感情音声の合成を志向してその第一歩として感情音声の知覚モデルを構築した。このモデルは三層構造であり、第１層は感情（怒り、喜び、悲しみ等）、第２層は第３層の音響特徴と第１層を結ぶ基礎的な心理量表現となっている。多次元尺度構成法およびファジイインターフェースシステムを用いて、各感情のモデル化を行った。三層構造とすることで、柔軟にモデル構築が可能となった。

図２：音源分離にもとづいた音声認識

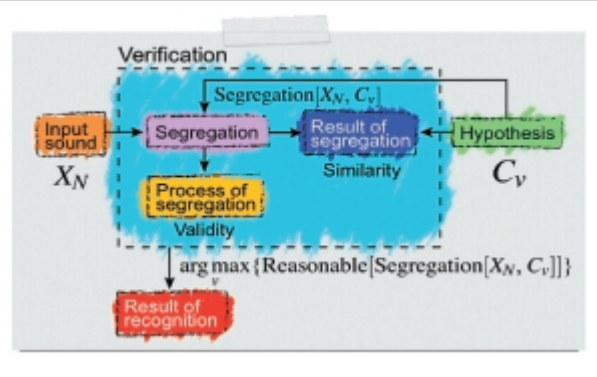


図３：歌声合成システム

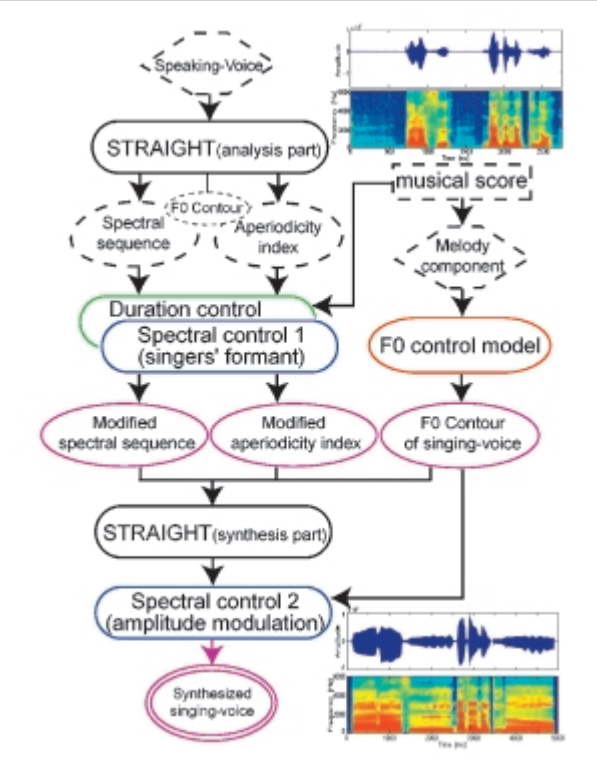


図４：感情（喜び）の知覚モデル

拠点形成に関連する主な業績

[1] Li, J. and Akagi, M. (2006). “A noise reduction system based on hybrid noise estimation technique and post-filtering in arbitrary noise environments,” Speech Communication, 48, 111-126.

[2] Haniu, A., Unoki, M. and Akagi, M. (2005). “A study on a speech recognition method based on the selective sound segregation in noisy environment,” Proc. NCSP05, Hawaii, 403-406.

[3] Saitou, T., Unoki, M. and Akagi, M. (2005). “Development of an F0 control model based on F0 dynamic characteristics for singing-voice synthesis,” Speech Communication 46, 405-417.

[4] Huang, C. F. and Akagi, M. (2005). “A Multi-Layer fuzzy logical model for emotional speech Perception,” Proc. EuroSpeech2005, Lisbon, Portugal, 417-420.

教授
党　建武
Dang, Jianwu
http://www.jaist.ac.jp/~jdang

研究グループ
電子社会のための安心基盤技術

専門分野
情報処理と電子社会の安全性

拠点形成における研究テーマ
人間のメカニズムを考慮した
高度ヒューマンインタフェース

研究の目指すもの

人を対象とした生体情報処理、マルチモダリティに対応したメディア処理を基盤技術として、人・電子社会および電子社会を媒体とした人・人間の安全な情報交換に必要なインターフェースの研究を行う。具体的には、生理学・心理学等との学際的協調による人間情報処理、マルチメディアを用いた電子社会との安全な相互アクセスシステムの構築、障害者支援ヒューマンインタフェースを物理エージェントとする共存インテリジェント空間の構築、これらをシミュレートするグリッドシステム技術、などの研究を行う。

マン・ツ・マンやマン・マシンのコミュニケーションにおいて言語音声による通信手段はわれわれ人間にとって最も自然である。これを実現するため音声合成・認識の技術を開発してきたが、その現状は社会的なニーズを満たすまでにはまだかなりの距離がある。音声認識では、理想的な環境で丁寧な発声に対してほぼ応用可能なレベルに達したが、雑音環境または感情を込めた音声に対してほとんど無能に近い。

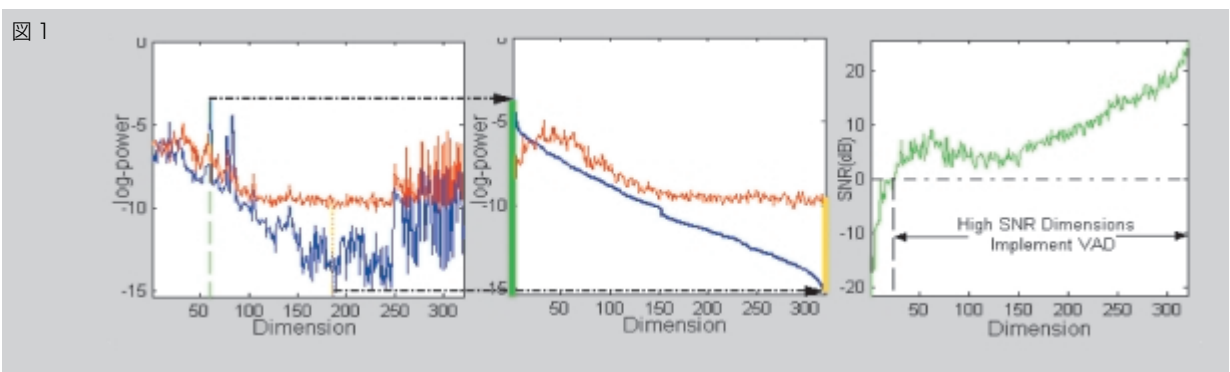
人間の脳内で音声の生成と知覚とを密接に結ぶ情報交換の通路（ことばの鎖）が存在するため、発話の感情や環境雑音などの影響により音声波形と発話の音素系列とのはっきりした対応関係は見られなくなるにもかかわらず、人間は問題なくそれらの対応関係を見つけ出すことができる。もし人間のこのような優れた音声生成・知覚の機能を究明して応用することができれば、上記の問題の根本的な解決を期待できると思われる。本研究では、計算モデルを用いて人間の音声生成と音声知覚の過程を模倣することによりそのメカニズムを究明し、あらゆる環境の下で頑健なコミュニケーションができる手法を開発することを目的とする。

拠点形成に関連する最近の研究テーマと成果

研究課題１：雑音環境に音声の検出方法について

雑音が音声に混入した場合、音声の検出が困難になる。図１の左パネルに示したように、信号雑音比が零である場合でも、一般的音声（赤）が雑音（青）より大きい区間が存在する。その区間の情報を利用して音声抽出の新しい手法を提案した。この手法では、前もって雑音毎の特性空間の分布を調査したうえ、雑音の特性ベクトルの大きい順でソートして、それに対応して音声を雑音の特性空間へ投影する。その結果、信号雑音比の高い成分が雑音特性空間の高次元領域に集中されることになる（中間と右のパネルを参照）。その領域の情報のみを使用することによって頑健に音声を検出することができる。

図１



研究課題２：人間のメカニズムに基づいた音声合成

音声によるコミュニケーションは人間が特有な機能である。音声生成過程では発話器官の動き・変形により空気通路を形成し、音声を生成する。発話器官の相互作用により調音結合が起こされ発話の自然さを増す。調音結合のモデル化と実現は、発話調音モデルを用いた音声合成器の構築にとって最も重要な課題である。本研究では、先行研究で構築した発話機構モデルを用い人間生成過程を模擬しながら、バイレベル学習法に基づいて「真」の調音目標をもとめ最適な調音結合モデルを作成する。生理学層では、モデルシミュレーションと観測データとの差を最小するように運動制御レベルにおける計画目標を学習する。ハイレベルでは、学習した計画目標を用いて調音結合モデルの係数を最適化する。学習した結果の一例を図２に示す。観測データは青でシミュレーション結果は赤で示し、黒いローマ字は学習した「真」の目標である。この実験ではこれまで仮設された「真」の目標を初めて実証した。

研究課題３：音声波から発話形状への逆問題について

語学の学習や難聴者の発話訓練などでは、音声波から発話状態を推測する必要がある。音声から発話状態へのマッピングは多意性をもつ逆問題である。その多意性を抑えるため、本研究では、まず生理学的３次元発話機構モデルを用いて調音筋空間を遍歴することにより可能な発話状態を生成した。その結果、60000 セットの調音・音響データを獲得した。発話状態は３次元モデルの舌上の 17 個の観測点で表し、発話状態に基づいた声道断面積関数から計算された第１、２ホルマント周波数は母音の音響特徴とした。日本語５母音に合わせて音響特性により発話状態を選択した。選択した発話状態の分布を分析したところ、一つの母音に対して、調音的に多峰性の分布となっていることを明らかにした。例として、母音 /u/ の分布を図３に示す。それにより、/u/ の発話で２つ異なる舌形状で実現することができる。

この研究結果を音声波から発話状態の逆推定に取り入れるため、混合ガウス分布モデルを用いて母音の調音分布をモデル化した。さらに、GGOF（Global measure of goodness of fit）を用いてモデルの適合度を評価することにより最適混合数を検討した。表１には各母音を表現するため適切な混合分布を示した。その結果、母音の発話状態の分布を反映する混合ガウス分布が得られた。

図２

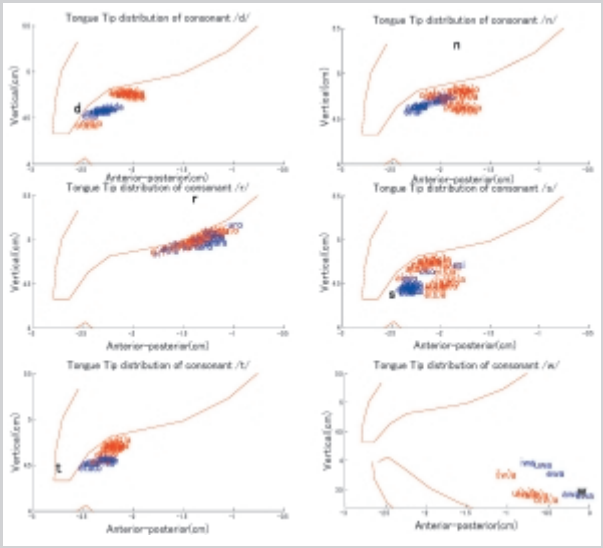


図３

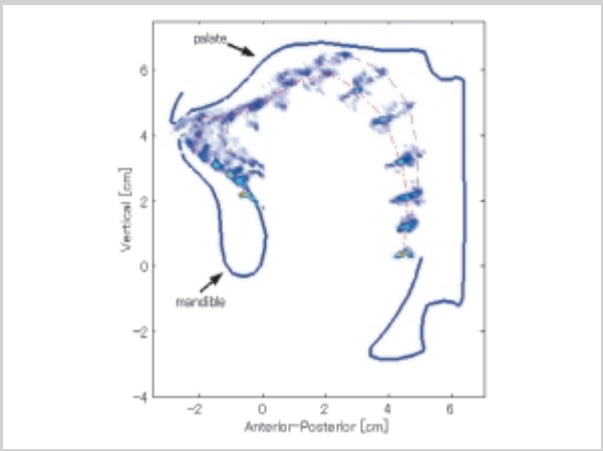


表１　各母音の最適混合分布

Vowel	/a/	/i/	/u/	/e/	/o/
Optimum mixture number	2	1	3	2	2
Weight coefficients for optimum mixture number	0.93 0.07	1.00	0.65 0.23 0.12	0.94 0.06	0.58 0.42
Maximum mixture number	6	2	10	11	3

拠点形成に関連する主な業績

[1] Ying, D.,Shi. Y.,Soong, and Dang, J (2006). “A Robust VAD based upon Noise Eigenspace Projection”, Proc. of Spring Meeting of The Acoustical Society of Japan, pp.147-148.
[2] Dang, J., Wei, J., Suzuki, T., Perrier, P (2005). “Investigation and modeling of Coarticulation during Speech,” Interspeech 2005，pp. 1025-1028 (Lisbon, Portugal)
[3] Wei, J., Lu, X.， and Dang, J. (2006). “Parameter optimization for a coarticulation model based on observation and simulation,” International Symposium of Frontiers in Speech and Hearing Research, pp.49-54.
[4] 錦戸信和，党建武 (2006).“モデルを用いた模擬に基づく発話状態の多意性の分析” 日本音響学会全国大会論文集，pp.261-262.

ポスドク研究員

Theorem Proving with Proof-Search and Counter-Model Construction

松本　利雅

研究内容

The aim of the present research is to develop a proof assistant system which facilitates theorem proving with proof and counter-model. From the practical point of view, it does not suffice to judge whether a given formula is provable or not only by checking a response, such as yes and no, from theorem prover, because such a response never tells us why the formula is provable or not. Therefore, we desire theorem proving such that it gives us a proof if a given formula is provable, otherwise it gives us a counter-model. As we expect, proof gives us a guarantee that a given formula is provable, while counter-model gives us an evidence which shows why the formula is not provable. Proof and counter-model enable us to check the correctness of theorem proving. We call a theorem prover which always returns either of proof or counter-model, proof assistant system. Our proof-search goes based on sequent system, that is our proof is given by sequent system, while our counter-model given by Kripke model can be constructed from failed proofs when proof-search fails. We can carry both proof-search and counter-model construction simultaneously.

Also, readability of proof is discussed. we should eventually judge the provability of given formulas with proof and counter-model. However, it is hard for us to read proofs from automatic proof-search, because auxiliary symbols required for tracking loops occur in the proofs. Such auxiliary symbols makes our proofs harder to read. In addition, not all applications of rules in the proofs are necessary. There is a high possibility that redundant applications are included in our proofs. Therefore, for the sake of readability of proof, it is required to reconstruct raw proof from automatic proof-search into proof we can read easily by eliminating auxiliary symbols, redundant applications of rules and so on. On the other hand, when we construct counter-model from failed proofs, some possible worlds are generated redundantly. As we expect, it is desired to reduce such a counter-model so that it would not have redundant possible worlds.

In the present research, we take up the basic 15 normal modal logics K, KD, KT, KB, KTB, KDB, K4, S4, K4D, K4B, K5, K5D, K45, K45D and S5, which are obtained from the least normal modal logic K by adding the following basic axioms: T($\Box A \supset A$), D($\Box A \supset \Diamond A$), B($A \supset \Box\Diamond A$), 4($\Box A \supset \Box\Box A$), 5($\Diamond A \supset \Box\Diamond A$), where $\Diamond$ is an abbreviation of $\neg\Box\neg$. Although the 32(=2^5) normal modal logics are obtained by combining the axioms, the logical equivalence reduces them to the above basic 15 normal modal logics. For the purpose of providing proof-search for the modal logics, we first need a decision procedure for each logic, which judges whether a given formula is provable or not, and gives us a proof of the formula if it is provable. Such a procedure is called proof-search procedure. Our proof-search procedure is given by sequent system. The first thing we have to do is to propose sequent systems which are suitable for proof-search for the 15 modal logics, such that they can avoid loops in proof-search efficiently. So far, technique for proof-search for modal logics, such as introducing cut-free proof systems, introducing auxiliary symbols and restricting on the form of cut formulas, have been proposed. Such techniques are useful to reduce the range of search of proofs and enables us to have efficient proof-search. We also have to formalize procedure for constructing counter-model from failed proofs for each logic.

Here, we must say the Tableaux Work Bench, called TWB for short, developed by P. Abate at RSISE, ANU. The TWB allows the user to define tableau or sequent rules together with a strategy for applying these rules. The TWB compiles this information into a proof-searcher for the given rules. The user can design sophisticated rules and strategies by utilizing various features of the TWB like history mechanism for tracking loops, starring mechanism for marking formulas and so on. The TWB enables us to carry out systematic implementation for the 15 modal logics. As for readability of proof and counter-model, we must say the X windows system Proof Editor, called XPE for short, developed by M. Mouri at JAIST. The XPE uses LaTeX as the underlying communication technology and displays proof by interpreting LaTeX commands so that the user can get WYSIWYG. The integration of the TWB and the XPE plays a vital role in this research.

ポスドク研究員

Transforming Nature Language Sentence to Logical Form

NGUYEN, Minh Le

研究内容

We have developed two methods for transforming a NL sentence to a logical form. The first one is applied maximum entropy models to learn from the corpus of sentences and logical forms. This method is applied for the problem of transforming query sentences to SQL language and it shows a good performance on that corpus. However, it required designing a set of features for maximum entropy models. In order to find a better model that minimizes the effort on designing features, we have developed a second method for transforming NL sentences to LF that is based on structured classification. This method shows a very good performance when exploited it in the corpus of robot soccer language (CLANG). These results indicated that it could be well suitable for the problem of transformation NL to LF. The main idea of this method is to represent LF as structured data and then applied a structured support vector machine model to deal with the structured prediction problem. There are three processes for transforming NL sentence to LF. The first process, namely semantic tagging, is to tag a given input sentence to a sequence of lexical meaning. The second one is to parse the output obtained from the first part to a semantic tree by using a structured support vector machine model. In final, the logical form is generated by simply using a bottom up method on the semantic tree. For the semantic tagging, we applied a conditional random field model and obtained a very high accuracy (98%) on a published corpus. For the semantic parsing problem, we obtained a very high result in comparison with previously published works. We reported the result in our publication in which our method achieved the best precision obtained in the published corpus.

We developed several new techniques for improving the performance of conditional random field models. The first one is applied association rule to mine the rare but importance rule for improving the chunking task. We also applied this tool for the task of semantic tagging that mapping each word in sentence to a lexical semantic meaning. The results show the performance is very high. To deal with the problem of large scale data, we developed a parallel version of high-order CRF models. It speeds up the performance to 90times in comparison with an original CRF model when testing on a full pen tree bank corpus. We also draw a semi-supervisor learning for CRF using co-training model and tested it on the CoNLL shared task corpus. It shows that the method can improve the performance of CRF itself. We also are interested in the problem of text summarization and its application to legal domain. We designed a new sentence extraction model which is based on an ensemble technique for support vector machine models. We are also interested in the task of named entities recognition with a semi-supervised learning method using a bootstrapping technique. In addition, we also published a freely a toolkit for both sequential conditional random fields and a parallel conditional random filed models. It is now the open source code software with very good performances when testing on various tasks, from text chunking to pos tagging tasks.

ポスドク研究員

Theory-based Legal Argumentation with Additive Consolidation

鈴木　義崇

研究内容

Our aim is to supply a formal tool which accounts theory-based legal argumentation, where theory means a set of rules intended to provide an account of legal domain. In this paper, We consider that this argumentation is performed as follows. At first, the proponent constructs a coherent theory, which derives the winning statement for him. Second, because the opponent cannot accept the first theory as coherent, he adds some information to this theory, and constructs a coherent theory, which defeats the winning statement for the proponent. Third, because the proponent cannot accept the second theory as coherent, he adds some information to this theory, and constructs a coherent theory, which derives the winning statement for him, and so on. In Suzuki and Tojo (2005), we used a variation of Olsson's additive consolidation (1998), which adds some information to incoherent knowledge and makes the knowledge coherent, and applied it to the formalization of a dialogue game about Bench-Capon and Sartor's example (2001, 2002, 2003), but this dialogue game was not treed, because, in each move on the dialogue, the consolidation must construct a unique coherent theory, but not several coherent theories. Therefore, we will accept Doyle's discussion (1991) about belief revision and solve the problem about the uniqueness. He proposed a variation of AGM's original belief revision (1995). Whereas AGM's revision is a deterministic function, which accepts an original theory and an incorporated external information, and generates a unique revised theory, his belief revision is a nondeterministic function, which accepts an original theory and an incorporated external information, and generates a set of the best alternative revised theories. In the same way, we repair the two deterministic consolidations in Suzuki and Tojo (2005), which accept an original theory and proponent's winning statement, and generate a unique consolidated theory, and introduce the nondeterministic consolidation, which accepts an original theory and proponent's winning statement, and generates a set of the best alternative consolidated theories. Such an expansion of the consolidations enable us to formalize a dialogue game tree about Bench-Capon and Sartor's example. Moreover, we can propose rational postulates of the nondeterministic consolidation, and prove the representation theorem between the operational function and the rational postulates. In future work, we will study the strategical aspect of the game tree with the framework of game theory.

ポスドク研究員

High Level Synthesis of Ultra High Performance Asynchronous Systems

大橋　功治

研究内容

As a VLSI system becomes larger and the clock period becomes shorter, it becomes difficult to control a digital circuit by a global clock under the fluctuation of datapath delay and clock skew. Asynchronous design is considered as a promising alternative, since it is free from such a global clock. Also it has the potential to achieve low power consumption, higher average-case performance, and higher reliability. To design a cost effective high performance asynchronous system for a specified application, optimization of datapath in register transfer level is an important design step. Scheduling and resource binding (assignment) are major subtasks in datapath synthesis not only for synchronous systems but also for asynchronous systems.

In this work we propose a synthesis system, which can generate asynchronous datapaths having good statistical performances. Now, we consider the problem to find a datapath and a schedule with minimum mean total computation time with maximum total computation time under given set of available modules and the upper bound of maximum total computation time. The proposed algorithm is summarized as follows. Basically, one operation (data), which is not assigned yet, and one functional unit (register) in given available modules are selected, and the operation (register) is assigned to the functional unit (register). Then the unambiguous sequences of operations and data, which are induced by this resource assignment, are fixed. Finally, when all operation and data are assigned to functional units and registers, all unresolved sequentializations are fixed.

The proposed algorithm is implemented using C program language on a 1GHz Pentium III personal computer. Experimental results shows solutions with the maximum 2.14 % reduced mean total computation time by comparison with the conventional systems. Also it shows our system runs about maximum 147.57 times faster than the conventional ones.

構成員（平成18年4月現在）

（1）拠点リーダー

片　山　卓　也	情報科学研究科・情報システム学専攻	教　授

（2）事業推進担当者

● **電子社会のための法令文書論理表現と推論グループ**

島　津　　明	情報科学研究科・情報処理学専攻	教　授
東　条　　敏	情報科学研究科・情報処理学専攻	教　授

● **電子社会のための形式推論機構グループ**

小　野　寛　晰	情報科学研究科・情報処理学専攻	教　授
小　川　瑞　史	安心電子社会研究センター	特任教授
VESTERGAARD, Rene	情報科学研究科・情報システム学専攻	助教授

● **電子社会のための形式検証技術グループ**

二　木　厚　吉	情報科学研究科・情報システム学専攻	教　授
平　石　邦　彦	情報科学研究科・情報システム学専攻	教　授
BJØRNER, Dines	情報科学研究科・情報処理学専攻	特任教授
緒　方　和　博	情報科学研究科・情報処理学専攻	特任助教授
青　木　利　晃	安心電子社会研究センター	特任助教授

● **電子社会のためのモデル化技術グループ**

落　水　浩一郎	情報科学研究科・情報システム学専攻	教　授
池　田　　満	知識科学研究科・知識システム基礎学専攻	教　授
鈴　木　正　人	情報科学研究科・情報システム学専攻	助教授

● **電子社会のための安心基盤技術グループ**

篠　田　陽　一	情報科学センター	教授
DÉFAGO, Xavier	情報科学研究科	特任助教授
SHEN, Hong	情報科学研究科・情報システム学専攻	教授
宮　地　充　子	情報科学研究科・情報システム学専攻	助教授
双　紙　正　和	情報科学研究科	特任助教授
日比野　　靖	情報科学研究科・情報システム学専攻	教授
金　子　峰　雄	情報科学研究科・情報システム学専攻	教授
浅　野　哲　夫	情報科学研究科・情報処理学専攻	教授
赤　木　正　人	情報科学研究科・情報処理学専攻	教授
党　　建　武	情報科学研究科・情報処理学専攻	教授

（3）安心電子社会研究センター（TRUST）

センター長	片　山　卓　也	北陸先端科学技術大学院大学・情報科学研究科
特任教授	小　川　瑞　史	北陸先端科学技術大学院大学・安心電子社会研究センター
特任助教授	青　木　利　晃	北陸先端科学技術大学院大学・安心電子社会研究センター
客員教員	岩　井　　淳　助教授	群馬大学・社会情報学部
	堀　雅　　和　助教授	インテック・ウェブ・アンド・ゲノム・インフォマティック㈱
客員研究員	梅　村　晃　広	㈱ＮＴＴデータ
事務員	桜　井　美　幸	北陸先端科学技術大学院大学

研究員

	氏　　名	採用年度	研究室
ポスドク	松　本　利　雅	平成16年度	小野
	NGUYEN, Minh Le	平成16年度	島津
	鈴　木　義　崇	平成16年度	東条
	大　橋　功　治	平成17年度	金子
	矢　竹　健　朗	平成18年度	片山
博士学生研究員	林　信　宏（リン　シンコウ）	平成16年度	片山
	ZHANG, Yuanyuan	平成16年度	井口
	黄　　明　仁	平成16年度	片山
	錦　戸　信　和	平成16年度	党
	LI, Guoqiang	平成17年度	小川
	NGUYEN, Thai Phuong	平成17年度	島津
	CHEN,Yawen	平成17年度	Shen
	ZHANG, Haibo	平成17年度	Shen
	VU, Thang Tat	平成17年度	赤木
	CHEN, Fan	平成17年度	小谷
	SUN, Wei	平成17年度	井口
	RYU, Jae-Kwan	平成17年度	Chong
	NGUYEN, Thanh Tri	平成17年度	島津
	VO, Hieu Dinh	平成18年度（予定）	落水
	NGUYEN, Tang Van	平成18年度（予定）	小川
	NGUYEN, Vinh Van	平成18年度（予定）	島津
	FANG, Qiang	平成18年度（予定）	党
	NGUYEN, Tien Lan	平成18年度（予定）	篠田
	YANG, Yan	平成18年度（予定）	Défago

過去の研究員

ポスドク	清　野　貴　博	平成17年度	二木
博士学生研究員	白　勢　政　明	平成16-17年度	日比野
	黄　　純　芳	平成16-17年度	赤木
	小　畑　貴　之	平成16-17年度	金子
	QU, Wenyu	平成16-17年度	Shen
	TIAN, Hui	平成16-17年度	Shen
	梅　田　　梢	平成16-17年度	宮地
	早稲田　篤　志	平成16-17年度	宮地
	寺　田　剛　陽	平成16-17年度	宮地
	中　田　潤　也	平成16-17年度	丹
	矢　竹　健　朗	平成17年度	片山
	XIONG, Naixue	平成17年度	Défago

アドバイザー委員会

- 辻　井　重　男　　情報セキュリティ大学院大学学長
- 玉　井　哲　雄　　東京大学大学院　総合文化研究科教授
- 木　下　佳　樹　　産業技術総合研究所　システム検証研究センター長
- 新　田　克　己　　東京工業大学大学院　総合理工学研究科教授
- 松　本　隆　明　　NTT データ技術開発本部長

外部機関との連携体制

国 内

（1） NTT データ（株）…… 連携内容：企業情報システムの分析と検証
連携講座「電子社会システム学」の実施

（2）インテック・ウェブ・アンド・ゲノム・インフォマティックス㈱、富山県庁 …… 連携内容：富山県行政業務のための法推論システムとオブジェクトモデリング

（3）産業技術総合研究所 システム検証研究センター …… 連携内容：システム検証理論、検証方式

（4）NICT …… 連携内容：インターネットシミュレータとその応用

（5）電子商取引研究組合 …… 連携内容：セキュリティポリシーの形式検証

国 外

（1）AT&T Labs-Research …… 連携内容：高信頼情報システム構築法

（2）スイス連邦工科大学 …… 連携内容：分散システムの耐故障技術

（3）オーストラリア情報通信 COE …… 連携内容：形式的仕様記述のための論理と推論システム

（4）ミラノ工科大学 …… 連携内容：情報システムのモデル化と進化方法論

（5）マサチューセッツ大学 …… 連携内容：電子社会のシミュレーション

（6）デンマーク工科大学 …… 連携内容：形式方法論

イベント

(1) 国際会議・シンポジウム

2005/3/8	International Symposium on Communication and Software Technologies for Ubiquitous Computing, http://www.jaist.ac.jp/jaist-coe/jpn/conferences/symposia_list/20050308_communication_and_software_technologies.html
2005/3/10-11	JAIST 21 世紀 COE シンポジウム 2005 「検証進化可能電子社会」, http://www.jaist.ac.jp/jaist-coe/jpn/conferences/symposia_list/jaist_coe_symposium_2005_march.html
2006/3/8-9	JAIST 21 世紀 COE シンポジウム 2006 「検証進化可能電子社会」, http://www.jaist.ac.jp/jaist-coe/jpn/conferences/symposia_list/jaist_coe_symposium_2006_march.html

(2) ワークショップ

2004/9/27-10/1	Japan-Switzerland Joint Seminar on Reliable and Efficient Internet Large-Scale Systems (REILS 2004), Kanazawa
2004/10/18	COE Workshop on Modal and Substructural Logics
2005/1/26	COE Workshop on Logic and Algebra
2005/4/24 - 25	COE Workshop on Binding Challenges
2005/5/16 - 18	International Workshop on Discrete and Computational Geometry
2005/9/21 - 22	COE Workshop on Verification Technology for e-Society 2005
2005/11/28 - 29	定理証明系ミーティング（Theorem Proving Systems Meeting）

(3) セミナー・講演会

● COE セミナー

2005/4/27	COE セミナー : 産総研システム検証研究センター紹介
2005/4/28	COE セミナー : ISO/IEC15408 評価認証の概要と HEAL 証拠資料の形式化
2005/5/2	COE セミナー : Incremental Software Construction
2005/7/4-5	COE セミナー : Domain Engineering
2005/7/20	COE セミナー : Trusted Computing and Trustworthy Networks in Tsinghua University
2005/7/26	COE セミナー : Hierarchical Mobile IPv6 and Dynamic Hierarchy
2005/7/26	COE セミナー : Time synchronization in wireless sensor network
2005/9/29	COE セミナー : Higher-Order Rewriting: Examples, Framework, Confluence and Termination
2005/12/1	COE セミナー : 第 28 回 ソフトウェアコロキウム : Communciating Processes: overview of theory and applications
2006/1/13	COE セミナー : プロセス形式化技術の集団的意思決定問題への適用と社会進化の過程
2006/3/22	COE セミナー : Vega Grid: Research Problems and Technical Advances
2006/3/24	COE セミナー : Grid Research in China and Potential Cooperation with Japan

● **情報科学研究科セミナー**

16年度

2004/10/29	第 2 回 情報科学研究科セミナー：コーペスベース音声合成
2004/11/12	第 3 回 情報科学研究科セミナー：最近の共通鍵暗号とそのソフトウエア実装法について
2004/12/1	第 4 回 情報科学研究科セミナー：分子の核スピンを使った真の量子計算
2004/12/9	第 5 回 情報科学研究科セミナー：自然言語処理の二つのアプローチ、統計ベース（コーパスベース）vs. 規則ベース
2004/12/10	第 6 回 情報科学研究科セミナー：音楽情報処理が実世界と結び付く：あなたも使える音楽情報処理
2004/12/15	第 7 回 情報科学研究科セミナー：感性情報科学の現状と今後
2005/1/14	第 8 回 情報科学研究科セミナー：CMMIと企業におけるプロセス改善上の課題
2005/1/14	第 9 回 情報科学研究科セミナー：移動通信とセキュリティ
2005/1/18	第10回 情報科学研究科セミナー：ACツリーオートマトンとParikhの定理
2005/1/21	第11回 情報科学研究科セミナー：人間共存型ロボット技術
2005/2/8	第12回 情報科学研究科セミナー：電子文書・電子化文書の長期保存技術について～21世紀のパピルス～
2005/2/10	第13回 情報科学研究科セミナー：ストレージフュージョンとその応用としての巨大ウェブ空間解析、国立情報学研究所における情報アクセス技術の共同研究
2005/2/22	第14回 情報科学研究科セミナー：日本を指導する立場に立つであろう若い皆様に!
2005/2/23	第15回 情報科学研究科セミナー：オフセット印刷向けスクリーニング技術の基礎と最新技術の動向
2005/3/3	第16回 情報科学研究科セミナー：電子投票：プロトコルとシステム

17年度

2005/6/6	第 1 回 情報科学研究科セミナー：生命ソフトウェアを目指して
2005/6/7	第 2 回 情報科学研究科セミナー：ビジュアル言語Viscuit
2005/6/13	第 3 回 情報科学研究科セミナー：The Changing Face of Software Engineering Education
2005/6/29	第 4 回 情報科学研究科セミナー：研究用ヒューマノイドロボットHOAPを用いた生物規範の制御・認識研究
2005/7/4	第 5 回 情報科学研究科セミナー：Interactive Smart Computers
2005/7/12	第 6 回 情報科学研究科セミナー：オンラインパッキング問題とオンラインサーバー問題
2005/9/9	第 7 回 情報科学研究科セミナー：r進数非隣接形式（rNAF）とペアリング暗号への応用
2005/9/13	情報科学研究科セミナー：ヒューマノイドロボット上の自己増殖型ニューラルネットワークを用いた能動的・追加的概念獲得
2005/10/14	第 8 回 情報科学研究科セミナー：ヒューマノイドロボット
2005/11/16	第 9 回 情報科学研究科セミナー：デジタル放送の技術とサービス展開
2005/11/16	第10回 情報科学研究科セミナー：ロボット・セラピー
2005/12/19	情報科学研究科セミナー：オンデマンド情報抽出、及び、情報アクセス技術
2006/1/6	第11回 情報科学研究科セミナー：暗号と格子
2006/1/20	第12回 情報科学研究科セミナー：電気通信事業の変遷と最近の話題
2006/1/26	第13回 情報科学研究科セミナー：汎用連想計算エンジンGETAによる情報の発見
2006/2/17	第14回 情報科学研究科セミナー：ブロック暗号の線形解読法
2006/3/7	第15回 情報科学研究科セミナー：4Kデジタルシネマ技術とその応用
2006/3/8	第16回 情報科学研究科セミナー：OK量子化理論、画像処理アルゴリズムの近況とその周辺

● AL（Algorithm & Logic）セミナー

2004/10/14	第105回 AL セミナー : Introduction to algebraic logic
2004/10/21	第106回 AL セミナー : Many-dimensional logical systems, Spatio-temporal logics: expressiveness vs. complexity
2005/2/28	第107回 AL セミナー : Continuous Fraissé Conjecture
2005/5/31	第108回 AL セミナー : Temporal Logic over transitive states
2005/9/6	第109回 AL セミナー : A path order POP and its applications
2005/12/12	第110回 AL セミナー : Acts of Commanding and Changing Obligations
2006/1/20	第111回 AL セミナー : Belnap's 4-valued logic and logic programs verification
2006/2/10	第112回 AL セミナー : Some Problems of Early Indian Logic
2006/2/28	第113回 AL セミナー : Atomicity and formal semantics
2006/3/16	第114回 AL セミナー : Completeness of a Hypersequent Calculus for Some First-order Gödel Logics with Delta

● 情報セキュリティセミナー

2004/11/12	最近の共通鍵暗号とそのソフトウエア実装法について
2005/1/14	移動通信とセキュリティ
2005/3/3	電子投票：プロトコルとシステム
2005/5/6	Kleptography: The Outsider Inside Your Crypto Devices (and its trust implications)

● その他のセミナー

2005/4/4-6	離散幾何学と計算幾何学に関する国際セミナー

広報活動

- 「ノーベル賞級の成果を　21 世紀 COE 採択」北國新聞 2004 年 7 月 22 日付け朝刊 34 面
- 「競争率 11.4 倍　厳選　知の拠点」 読売新聞 2004 年 7 月 22 日付け朝刊 12 版 15 面
- 「21 世紀 COE プログラム」 週刊朝日 2004 年 10 月 22 日号 p112
- 「特別講演 情報科学による安心電子社会の実現」
  学際的情報セキュリティ総合シンポジウム 2004 年 11 月 23 日
- 「特集 21 世紀卓越した情報研究拠点プログラムの目指す研究（後編）」
  情報処理学会会誌 46 巻 5 号 , pp515-521, 2005
- 金沢大学・北陸先端科学技術大学院大学　第 5 回研究交流会　2005 年 12 月 12 日

発表論文

（1） 電子社会のための法令文書論理表現と推論

学術論文

Nguyen Minh Le, Susumu Horiguchi, Akira Shimazu, and Ho Tu Bao, "Example-based Sentence Reduction Using Hidden Markov Model," ACM Transactions on Asian Language Information Processing, Vol. 3, Issue 2, 146-158, June, 2004.

M. L. Nguyen, A. Shimazu, and S. Horiguchi, "A New Template Translation Learning Based on Hidden Markov Modeling," WSEAS Transaction on Computers, Volume 3, Issue 1, pp.256-262, 2004.

M. L. Nguyen and S. Horiguchi, "Accuracy Enhancement for the Decomposition of Human-Written Summary," International Journal of Computer Processing of Oriental Languages (IJCPOL), Vol.18, No.1, pp.53-74, 2005.

M. L. Nguyen, M. Fukushi, and S. Horiguchi, "A Probabilistic Sentence Reduction Using Maximum Entropy Model," IEICE Transactions on Information and Systems, Japan, Vol.E88-D, No.2, pp.278-288, 2005.

Cuong Anh Le, Akira Shimazu, and Van-Nam Huynh, "Word Sense Disambiguation by Combining Classifiers with an Adaptive Selection of Context Representation," Journal of Natural Language Processing, Vol.13, No.1, pp.75-95, 2006.

N. N. Tun and S. Tojo, "Unification of Sorts Among Local Ontologies for Semantic Web Applications," WSEAS Transactions on Computers, issue 2, Vol.4, pp.123-129, 2005.

国際会議

Nguyen Minh Le, Akira Shimazu, and Susumu Horiguchi, "Translation Template Learning Based on Hidden Markov Modeling," PACLIC17, 2003.

Nguyen Minh Le, Akira Shimazu, Susumu Horiguchi, Tu Bao Ho, and Masaru Fukushi, "Probabilistic Sentence Reduction Using Support Vector Machines," Coling2004, pp.743-749, Aug. 2004.

Nguyen Minh Le, Akira Shimazu, Tu Bao Ho, Susumu Horiguchi, and Xuan Hieu Phan, "A Cross-language Text Summarization Using Statistical Machine Learning," KSS'2004, Nov. 2004.

Cuong Anh Le and Akira Shimazu, "Improving Word Sense Disambiguiation Accuracy Using Naive Bayesian Classifier with Rich Features," KSS'004, Nov. 2004.

X. H. Phan, S. Horiguchi, T. B. Ho, and M. L. Nguyen, "An Unsupervised Approach to Coreference Resolution," 5th International Symposium on Knowledge and System Sciences, Ishikawa, Japan, Nov. 2004.

Kenji Takano and Akira Shimazu, "Analysis of Spoken Dialogues Based on Local Discourse Structures," KSS'2004, Nov. 2004.

Cuong Anh Le and Akira Shimazu, "High WSD Accuracy Using Naive Bayesian Classifier with Rich Features," PACLIC2004, Dec. 2004.

Cuong Anh Le, Van-Nam Huynh, and Akira Shimazu, "Combining Classifiers with Multi-Representation of Context in Word Sense Disambiguation," Tu Bao Ho, David Cheung, and Huan Liu (Eds.): Advances in Knowledge Discovery and Data Mining (LNAI 3518), pp.262-268, 2004. Proc. 9th Pacific-Asia Conference, PAKDD 2005, Hanoi, May 2005.

Cuong Anh Le, Van-Nam Huynh, and Akira Shimazu, "An Evidential Reasoning Approach to Weighted Combination of Classifiers for Word Sense Disambiguation," Petra Perner and Atsushi Imiya (Eds.) Machine Learning and Data Mining in Pattern Recognition (LNAI 3587), pp.516-525, 2005. Proc. 4th International Conference, MLDM 2005, Leipzig, Germany, July 2005.

Nguyen Minh Le, Akira Shimazu, and Hieu Xuan Phan, "Structured SVM Semantic Parser Augmented by Semantic Tagging with Conditional Random Field," 19th Pacific Asia Conference on Language, Information and Computation (PACLIC 19), pp.167-177, 2005.

Nguyen Minh Le, Akira Shimazu, and Hieu Xuan Phan, "A Maximum Entropy Model for Transforming Sentences to Logical Form," Shichao Zhang and Ray Jarvis (Eds.) AI2005: Advances in Artificial Intelligence (LNAI 3809), Springer, pp.800-804, 2005.

Nguyen Minh Le and Akira Shimazu, "Learning to Map Sentences to Formal Language with Structured SVM Classification: A Case Study for RoboCup Coach Langugage," 3rd International Conference on Computational Intelligence, Robotics and Autonomous Systems (CIRAS 2005), Singapore, Dec. 2005.

Y. Suzuki and S. Tojo, "Additive Consolidation for Dialogue Games," 10th International Conference on Artificial Intelligence and Law, 2005.

N. N Tun and S. Tojo, "IC-based Ontology Expansion in Devouring Accessibility," Australian Ontology Workshop (AOW), 2005.

S. Yoshioka and S. Tojo, "CB-CTL: A Reasoning System of Temporal Epistemic Logic with Communication Channel," 3rd International World Enformatika Conference, 2005.

S. Yoshioka and S. Tojo, "Many-dimentional Modal Logic of Tense and Temporal Interval and Its Decidability," 3rd International World Enformatika Conference, 2005.

K. Kaneiwa and S. Tojo, "Logical Aspects of Events: Quantification, Sorts, Composition and Disjointness," Australian Ontology Workshop (AOW), 2005.

Y. Suzuki and S. Tojo, "Additive Consolidation for Dialogue Games," 10th International Conference on Artificial Intelligence and Law, 2005.

S. Hagiwara and S. Tojo, "Stable Legal Knowledge with Regard to Contradictory Arguments," AIA: Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, 2006.

S. Yoshioka, M. Kobayashi, and S. Tojo, "State Updating of Channel Communication System CB/CTL," AIA: Proceedings of the IASTED International Conference on Artificial Intelligence and Applications, 2006.

その他（国内会議等）

M. L. Nguyen and A. Shimazu, "Transforming Natural Language Sentence to logical form (survey unpublished report)," 2004.

古田, 島津, "話し言葉による説明発話の特徴の分析と具体化について－格要素の語順に関して－," 言語処理学会第11回年次大会発表論文集, pp.273-276 , Mar. 2004.

江尻 暁, 北田安希雄, 島津 明, "法令文の論理式への変換－論理構造について－," 言語処理学会第12回年次大会, pp.4-9, 2006.

北田安希雄, 江尻暁, 島津明, "法令文の論理式への変換－原始文について－,"言語処理学会第12回年次大会, pp.4-10, 2006.

木村俊也, 中川晋一, 三角真, 山岡克式, 酒井善則, 島津明, "Web上のがん情報取得のためのがん用語辞書の作成," 言語処理学会第12回年次大会, pp.1-6, 2006.

嶋崎好文, 島津明, "ユーザと適応的に対話するための説明対話モデルについて,"言語処理学会第12回年次大会, pp.9-7, 2006.

山田大介, 島津明, "法令文の言語的特徴を利用した可読性向上のための表示,"言語処理学会第12回年次大会, pp.2-1, 2006.

吉岡卓, 東条敏, "時制と時区間を表現する複様相論理とその決定可能性,"人工知能学会誌, vol.21, No.3, 2006.

（2）電子社会のための形式推論機構

学術論文

Francesco Belardinelli, Peter Jipsen, and Hiroakira Ono, "Algebraic aspects of cut elimination," Studia Logica, Vol.77, No.2, pp.209-240, 2004

Mizuhito Ogawa, "Well-Quasi-Orders, and Regular Omega-languages," Theoretical Computer Science, Vol.324, No.1, pp.55-60, Words, Languages and Combinatorics, 2004.

Li Xin and Mizuhito Ogawa, "A Lightweight Mutual Authentication based on Proxy Certificate Trust List," Computer Software, Vol.22, No.2, pp.85-89, 2005.

Rene Vestergaard, "A Constructive Approach to Sequential Nash Equilibria," Information Processing Letters, 97, 2005.

国際会議

Hiroakira Ono, "Glivenko Properties of Substructural Logics, Residuated Structures and Many-Valued Logics," Patras, Greece, June, 2004.

Hiroakira Ono, "Completeness Problems of Predicate Logics around Goedel-Dummett Logic," The Challenge of Semantics, Vienna, Austria, July 12-17, 2004.

Mizuhito Ogawa, "Complete Axiomatization of an Algebraic Construction of Graphs," 7th International Symposium on Functional and Logic Programming, LNCS 2998, pp.163-179, 2004.

Hiroakira Ono, "Embeddings of Algebras and Their Logical Consequences," Trends in Logic III International Conference (invited talk), Warszawa/Ruciane-Nida, Poland, Sep. 2005.

Hiroakira Ono, "Interpolation Property and Principle of Variable Separation in Substructural Logics,", 9th Asian Logic Conference (invited talk), Novosibirsk, Russia, Aug. 2005.

Mizuhito Ogawa, Eiichi Horita and Satoshi Ono, "Proving Properties of Incremental Merkle Trees," 20th International Conference on Automated Deduction, CADE-20, Springer LNAI 3632, pp.424-440, 2005.

Isao Sasano, Mizuhito Ogawa, and Zhenjiang Hu, "Maximum Marking Problems with Accumulative Weight Functions," International Colloquium on Theoretical Aspects of Computing, ICTAC05, LNCS 3722, pp.562-578, 2005.

Li Xin and Mizuhito Ogawa, "Interprocedural Program Analysis for Java based on Weighted Pushdown Model Checking," accepted to 5th International Workshop on Automated Verification of Infinite-State Systems (AVIS'06), to appear in ENTCS.

その他（国内会議等）

小野寛晰, "論理的方法と代数的方法," 第二回システム検証の科学技術シンポジウム（招待講演), 大阪, Oct. 2005.

Guoqiang Li, Bochao Liu, Xin Li and Mizuhito Ogawa, "Type-directed Trace Analysis of Security Protocols in Process Calculus," 第22回日本ソフトウェア科学会大会 5A-3, Sept. 2005.

Masahiro Kitagawa, Akira Kataoka, and Mizuhito Ogawa, "Logarithmic Width Enumerative Coding," 第28回情報理論とその応用シンポジウムSITA2005予稿集, Vol.II, pp.395-398, Nov. 2005.

（3）電子社会のための形式検証技術

学術論文

片山卓也, "発展ドメイン：ソフトウェア発展のための理論的枠組み," コンピュータソフトウェア, Vol.21, No.3, pp.11-21, 2004.

青木利晃, 片山卓也, オブジェクト指向分析モデルにおけるデータフローの形式化と解析手法, 日本ソフトウェア科学会 学会誌 コンピュータソフトウェア, Vol.21, No.4, pp.1-26, 2004.

Kunihiko Hiraishi, Deriving Discrete Behavior of Hybrid Systems under Incomplete Knowledge, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E87-A, No.11, pp.2913-2918, 2004.

Takuya Katayama, Tatsuo Nakajima, Taichi Yuasa, Tomoji Kishi, Shin Nakajima, Shuichi Oikawa, Masahiro Yasugi, Toshiaki Aoki, Mitsutaka Okazaki, and Seiji Umatani, "Highly Reliable Embedded Software Development Using Advanced Software Technologies," IEICE Transactions on Information and Systems, Vol.E88-D, No.6, pp.1105-1116, 2005.

矢竹健朗, 青木利晃, 片山卓也, "コラボレーションに基づくオブジェクト指向モデルの検証,"コンピュータソフトウェア, Vol.22, No.1, pp.58-76, 2005.

岡崎光隆, 青木利晃, 片山卓也. "並行オブジェクトから並行処理列への変換法,"コンピュータソフトウェア, Vol.22, No.2, pp.58-73, 2005.

片山卓也, "特集 21世紀卓越した情報研究拠点プログラムの目指す研究（後編）：検証進化可能電子社会," 情報処理学会会誌, 46巻5号, pp.515-521, 2005.

中村正樹, 緒方和博, 二木厚吉, "項書き換えシステムにおける可簡約演算子とその応用,"情報処理学会論文誌：プログラミング, vol. 46, No.SIG6 (PRO25), pp.47-59, 2005.

Takahiro Seino, Kazuhiro Ogata, and Kokichi Futatsugi, "Mechanically Supporting Case Analysis for Verification of Distributed Systems," Journal of Pervasive Computing and Communications, Vol.1, No. 2, pp.135-145, 2005.

Jing Tian, Yoshiteru Nakamori, Jianwen Xiang, and Kokichi Futatsugi, "Knowledge Management in Academia: Survey, Analysis and Perspective,"Int. J. Management and Decision Making, Vol. 7, Nos. 2/3, pp. 275-294, 2006.

国際会議

Kenro Yatake, Toshiaki Aoki, and Takuya Katayama, "Collaboration-based Verfication of Object-Oriented models in HOL," 2nd International Workshop on Verification and Validation of Enterprise Information Systems, VVEIS 2004, pp.78-80, 2004.

Toshiaki Aoki and Takuya Katayama, "Foundations for Evolutionary Construction of State Transition Models," The Seventh International Workshop on Principles of Software Evolution, pp.143-146, 2004.

Tomoji Kishi, Toshiaki Aoki, Shin Nakajima, Natsuko Noda, and Takuya Katayama, "Project Report: High-Reliable Object-Oriented Embedded Software Design," 2nd IEEE Workshop on Software Technologies for Embedded and Ubiquitous Computing Systems (WSTFEUS), 2004.

Naohiro Hayashibara, Xavier Defago, Rami Yared, and Takuya Katayama, "The ϕ Accrual Failure Detector," 23rd IEEE International Symposium on Reliable Distributed Systems (SRDS-23), Florianopolis, Brazil, pp.66-78, Oct. 2004.

Peter Urban, Naohiro Hayashibara, Andre Schiper, and Takuya Katayama, "Performance Comparison of a Rotating Coordinator and a Leader Based Consensus Algorithm," 23rd IEEE International Symposium on Reliable Distributed Systems (SRDS-23), Brazil, pp.4-17, Oct. 2004.

Nguyen Truong Thang and Takuya Katayama, "Handling Consistency of Software Evolution in an Efficient Way," International Workshop on Principles of Software Evolution (IWPSE), pp.121-130, 2004.

Chaiwat Sathawornwichit and Takuya Katayama,"A Parametric Model Checking Approach for Real-Time Systems Design," Asia Pacific Conference on Software Engineering (APSEC05), pp.584-594, 2005

Kenro Yatake, Toshiaki Aoki, and Takuya Katayama, "Implementing Application-Specific Object-Oriented Theories in HOL," Theoretical Aspect of Computing - ICTAC2005, pp.516-516, 2005.

Toshiaki Aoki and Takuya Katayama, "Formalization and Analysis of Dataflow in Object-Oriented Design Models," International Symposium on Object-Oriented Real-Time Distributed Computing 2005, pp.95-105, 2005.

Ming-Jen Huang and Takuya Katayama, "Steering Model-Driven Development of Enterprise Information System through Responsibilities," WSMDEIS 2005, INSTICC Press, Portugal, pp.165-170, 2005.

Ming-Jen Huang and Takuya Katayama, "Steering Model-Driven Evolution by Responsibilities," IWPSE 2005, 2005.

Nguyen Truong Thang and Takuya Katayama, "A Formal Approach Facilitating the Evolution of Component-Based Software," International Workshop on Principles of Software Evolution (IWPSE2005), pp.49-52, 2005.

Nguyen Truong Thang and Takuya Katayama, "Constructing Open Systems via Consistent Components," International Colloquium on Theoretical Aspects of Computing (ICTAC2005), pp.517-531, 2005.

Nguyen Truong Thang and Takuya Katayama, "Specification and Verification of Inter-Component Constraints in CTL," Specification and Verification of Component-Based Systems Workshop (SAVCBS2005), Microsoft Research, pp.15-22, 2005.

Yasser Kotb and Takuya Katayama, "Consistency Checking of UML Model Diagrams Using the XML Semantics Approach," 14th International World Wide Web Conference 2005 (WWW2005), Chiba, Japan, pp.982-983, May 2005.

Yasser Kotb and Takuya Katayama, "A Consistency Checker for UML Model Diagrams," Workshop on Dependable Software - Tools and Methods, Joined with The International Conference on Dependable Systems and Networks (DSN-2005), pp. 192-197, Yokohama, Japan, June 2005.

Yasser Kotb and Takuya Katayama, "A Novel Technique to Verify the UML Use Case Diagrams," IASTED International Conference on Software Engineering (SE 2006), Innsbruck, Austria, pp.300-305, Feb. 2006.

Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi, "Model-Checking Observational Transition System with Maude," 20th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2005), pp.5-6, July 2005.

Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi, "Formal Analysis of Workflow Systems with Security Considerations," 17th International Conference on Software Engineering and Knowledge Engineering (SEKE 2005), pp.531-536, July 2005.

Masaki Nakamura, Masahiro Watanabe, and Kokichi Futatsugi, "A Behavioral Specification of Imperative Programming Languages," 2005 International Technical Conference On Circuits/System, Computers and Communications (ITC-CSCC 2005), pp. 403-404, July 2005.

Kokichi Futatsugi, Joseph Goguen, and Kazuhiro Ogata, "Verifying Design with Proof Scores," 1st IFIP-WG2.3 Conference on Verified Software: Tool, Theory, and Experience (electric form), Oct. 2005.

Weiqiang Kong, Kazuhiro Ogata, Takahiro Seino, and Kokichi Futatsugi, "A Lightweight Integration of Theorem Proving and Model Checking for System Verification," 12th Asia-Pacific Software Engineering Conference (APSEC 2005), IEEE CS Press, pp.59-66, Dec. 2005.

Masahiro Nakano, Kazuhiro Ogata, Masaki Nakamura, and Kokichi Futatsugi, "Automatic Verification of the STS Authentication Protocol with Creme," 20th International Technical Conference on Circuits/Systems, Computers and Communications (20th ITC-CSCC), pp.15-16, 2005.

Kazuhiro Ogata and Kokichi Futatsugi, "Equational Approach to Formal Analysis of TLS," 25th International Conference on Distributed Computing Systems (25th ICDCS), pp.795-804 2005.

Kazuhiro Ogata and Kokichi Futatsugi, "Proof Score Approach to Verification of Liveness Properties," 17th International Conference on Software Engineering and Knowledge Engineering (17th SEKE), pp.608-613, 2005.

Kazuhiro Ogata and Kokichi Futatsugi, "Analysis of the Suzuki-Kasami Algorithm with SAL Model Checkers," 5th International Conference on Computer and Information Technology (5th CIT), pp.937-943, 2005.

Kazuhiro Ogata, Masahiro Nakano, Masaki Nakamura, and Kokichi Futatsugi "Chocolat/SMV: A Translator from CafeOBJ into SMV," 6th International Conference on Parallel and Distributed Computing, Applications and Technologies (6th PDCAT), pp.416-420, 2005.

Kazuhiro Ogata and Kokichi Futatsugi, "Analysis of the Suzuki-Kasami Algorithm with the Maude Model Checker," 12th Asia-Pacific Software Engineering Conference (12th APSEC), pp.159-166, 2005.

Jittisak Senachak, Takahiro Seino, Kazuhiro Ogata and Kokichi Futatsugi, "Provably Correct Translation from CafeOBJ into Java," 17th International Conference on Software Engineering and Knowledge Engineering (17th SEKE), pp.614-619, 2005.

Takahiro Seino, Kazuhiro Ogata, and Kokichi Futatsugi, "A Toolkit for Generating and Displaying Proof Scores in the OTS/CafeOBJ Method," 6th International Workshop on Rule-Based Programming (6th RULE), ENTCS, Elsevier, 2005.

Jianwen Xiang, Kazuhiro Ogata and Kokichi Futatsugi, "Formal Fault Tree Analysis of State Transition Systems," 5th International Conference on Quality Software (5th QSIC), pp.124-131, 2005.

Kunihiko Hiraishi and Sunseong Choe, "Computational Tools for Designing Hybrid Systems Based on Constraint Satisfaction," Workshop on Control of Hybrid and Discrete Event Systems, Satellite workshop of ATPN2005, 41-60, June 2005.

Kunihiko Hiraishi, "Modeling and Verification of e-Society using DES Technology," SICE Annual Conference 2005, pp.2808-2811, July 2005.

Sunseong Choe and Kunihiko Hiraishi, "Application of Quantifier Elimination to Optimal Control Problems of Hybrid Systems," 7th Asian Symposium on Computer Mathematics, pp.62-65, Dec. 2005.

その他（国内会議等）

青木利晃, "オブジェクト指向モデルのための検証ツールの実装について," 情報処理学会 ソフトウェア工学研究会 Winter Workshop 2004ポジションペーパー, pp.7-8, 2004.

平石邦彦, 石川礼, "制約論理プログラミングによるハイブリッドシステムのパラメータ設計," 第17回回路とシステム軽井沢ワークショップ, pp.597-602, 2004.

青木利晃, 片山卓也, "アクション言語と制約言語を用いて記述されたオブジェクト指向設計モデルの検証法,"日本ソフトウェア科学会 第2回ディペンダブルソフトウェア研究会 (DSW2005), pp.61-70, 2005.

青木利晃, 片山卓也, "RTOSに基づいたソフトウェアのためのモデル検査ライブラリ,"組込みソフトウェアシンポジウム2005, pp.56-63, 2005.

青木利晃, 片山卓也, "ステートチャートに基づいたオブジェクト指向設計モデルの検証," FOSE2005, pp.55-64, 2005.

中村正樹, 二木厚吉, "モジュラーな代数仕様言語のための項書き換えシステム,"第二回システム検証の科学技術シンポジウム, pp. 106-121, Oct. 2005.

Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi, "Formal Modeling and Verification of Workflows with Security Considerations," 2nd Symposium on Science and Technology for System Verification, pp.135-149, Oct. 2005. （第二回システム検証の科学技術シンポジウム）

J. Xiang, K. Ogata, W. Kong, and K. Futatsugi, "From Safety Analysis to Formal System Specification and Verification with OTS/CafeOBJ," 2nd Symposium on Science and Technology for System Verification, pp. 64-78, Oct. 2005. （第二回システム検証の科学技術シンポジウム）

平石邦彦, 崔舜星, "制約充足に基づいたハイブリッドシステム設計のための計算ツール,"第18回回路とシステム軽井沢ワークショップ, pp.287-298, Apr. 2005.

崔舜星, 平石邦彦, "ハイブリッドシステムにおける最適制御問題へのQEの適用," 第15回インテリジェントシステムシンポジウム, 計測自動制御学会, pp.177-192, 2005.

平石邦彦, 小谷正行, "確率ペトリネットを用いたワークフローの性能評価," 計測自動制御学会システム・情報部門学術講演会2005, pp.354-359, Nov. 2005.

（4）電子社会のためのモデル化技術

学術論文

池田 満，林 雄介, "知の創造・継承のモデル化と支援システムのデザイン," ヒューマンインタフェース学会誌・論文誌　学習・創造・インタラクション特集，Vol. 6，No.2，pp. 19-26，2004.

国際会議

Saw Sanda Aye, Yi Zhou, and Koichiro Ochimizu, "Process Model Combining the Artifact Centered Process with Communication Path," The 5th International Workshop on Software Process Simulation and Modeling (ProSim 2004), May 2004.

Satoshi Hattori and Koichiro Ochimizu, "A Mathematical Foundation to Validate Some Empirical Organizational Patterns," International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA 2004), Vol.II, pp.95-101, July. 2004.

Pimruang Adirake, Kazuhiro Fujieda, and Koichiro Ochimizu, "Integration of Component-Based Development-Deployment Support for J2EE Middleware," 4th International Workshop on Software Engineering and Middleware (SEM 2004), Sept. 2004.

Masayuki Kotani and Koichiro Ochimizu, "Generating Dependency Relationships among UML Model Elements for Impact Analysis of UML Documents," 8th International Symposium on Future Software Technology (ISFST 2004), Oct. 2004.

M. Ikeda, Y. Hayashi et al., "Intellect Disclosure Support Based On Organizational Intellect Model," International Semantic Web Conference 2004 Workshop on Applications of Semantic Web Technologies for E-learning, 2004.

Koichiro Ochimizu, "Software Architecture with Accountability and Evolvability," JAIST 21st Century COE Symposium 2005 Verifiable and Evolvable e-Society, Mar. 2005.

W. Lu and M. Ikeda, "An Intention-oriented Model of Copyright Law for e-Learning: International Semantic Mapping of Copyright Laws Based on A Copyright Ontology," International Conference on Computer and Education 2005, pp.753-756, 2005.

その他（国内会議等）

朱霊宝, 池田満, 落水浩一郎, "ソフトウェア工学知識の体系化と管理法に関する一接近," 情報処理学会第145回ソフトウェア工学研究会, Aug. 2004.

Saw Sanda Aye, Mitsuru Ikeda, and Koichiro Ochimizu, "Defining Ontology for Complexity Issues in Software Engineering," 日本ソフトウェア科学会第21回大会, Sept. 2004.

早坂良, 藤枝和宏, 落水浩一郎, "電子大学の履修管理システムを対象とした自己説明性および進化容易性を実現するためのソフトウェア構成手法の検討," JAIST Research Report, IS-RR-2005-005, ISSN 0918-7553, Mar. 2005.

小谷正行, 落水浩一郎, "依存関係を用いた UML 文書間の波及解析法," 電子情報通信学会ソフトウェアサイエンス研究会, SS2004-62, Mar. 2005.

金旭東, 早坂良, 小谷正行, 落水浩一郎, "メタパターンを用いたJavaソースコードにおける協調クラス群の抽出," 情報処理学会ソフトウェア工学研究会, 情処研報2005-SE-150, pp.101-108, Nov. 2005.

早坂良, 堀雅和, 藤枝和宏, 落水浩一郎, "アカウンタビリティおよび進化容易性を持つソフトウェアアーキテクチャと3層モデルとの対応," 情報処理学会ソフトウェア工学研究会, 情処研報2005-SE-150, pp.1-8, Nov. 2005.

早坂良,　藤枝和宏,　落水浩一郎, "アカウンタビリティおよび進化容易性を持つ履修管理システムの設計," 日本ソフトウェア科学会 第 22 回大会, CD-ROM, Sept. 2005.

早坂良, 藤枝和宏, 落水浩一郎, "履修管理システムにおけるアカウンタビリティおよび進化容易性を実現するソフトウェアアーキテクチャ," 電子情報通信学会ソフトウェアサイエンス研究会, 信学技報 SS2005-32, pp.49-54, Aug. 2005.

服部哲, 落水浩一郎, "確率ペトリネットによる組織パターンの検証," コンピュータソフトウェア, Vol.23, No.1, pp.60-68, 2006.

早坂良、落水浩一郎, "履修管理システムにおけるオントロジを用いたアカウンタビリティ設計手法," 情報処理学会ソフトウェア工学研究会, 情処研報2005-SE-151, Mar. 2006.

小谷正行, 落水浩一郎, "ソフトウェア共同開発におけるワークフロー実行制御の一方式," 電子情報通信学会ソフトウェアサイエンス研究会, 信学技報SS2005-88, pp.31-36, Feb. 2006.

早坂良, 藤枝和宏, 落水浩一郎, "履修管理システムにおけるアカウンタビリティおよび進化容易性を実現するソフトウェアアーキテクチャ," 電子情報通信学会ソフトウェアサイエンス研究会, 信学技報, SS2005-32, pp.49-54, Aug. 2005.

早坂良, 藤枝和宏, 落水浩一郎, "アカウンタビリティおよび進化容易性を持つ履修管理システムの設計," 日本ソフトウェア科学会 第22回大会, CD-ROM, Step. 2005.

金旭東，早坂良，小谷正行，落水浩一郎， "メタパターンを用いたJavaソースコードにおける協調クラス群の抽出," 情報処理学会ソフトウェア工学研究会，情処研報2005-SE-150 pp.101-108，Nov. 2005.

早坂良，堀雅和，藤枝和宏，落水浩一郎，"アカウンタビリティおよび進化容易性を持つソフトウェアアーキテクチャと3層モデルとの対応," 情報処理学会ソフトウェア工学研究会，情処研報2005-SE-150，pp.1-8，Nov. 2005.

(5) 電子社会のための安心基盤技術

学術論文

田村裕子, 塩月徹, 宮地充子, "効率的な代理入札システム," 電子情報通信学会誌, Vol. J87-A, No.6, pp.835-842, 2004.

T. Terada, M. Soshi, and A. Miyaji, "Pushback機構の一提案とそのモデル化に向けて," IPSJ Trans., Vol.45, No.8, pp.1948-1953, 2004.

Shigeki Kitazawa, Masakazu Soshi, and Atsuko Miyaji. "On anonymity metrics for practical anonymous communication protocols," IPSJ Journal, Vol.45, No. 8, Aug. 2004.

Haibin Kan and Hong Shen, "A Note on Tanner Graphs for Group Block codes and Lattices," IEICE Transactions on Fundamentals, Vol.E87-A, No.8, pp.2182-2184, 2004.

J. Li, H. Shen, and R. Topor, "Mining informative rule set for prediction," Journal of Intelligent Information Systems, Vol.22, No.2, pp.155-174, 2004.

A. C. Leung, J. Sum, H. Shen, J. Wu, and G. H. Young, "Analysis and design of an agent searching algorithm for e-marketplaces," Cluster Computing , Vol.7, No.1, pp.85-90, 2004.

Keqiu Li and Hong Shen, "Optimal Proxy Placement for Coordinated En-Route Transcoding Proxy Caching," IEICE Trans. on Information and Systems, Vol.E87-D, No.12, pp.2689-2696, 2004.

Keqiu Li and Hong Shen, "Proxy Placement Problem for Coordinated En-Route Transcoding Proxy Caching," International Journal of Computer Systems, Science and Engineering, Vo.19, No.5, 95-103, 2004.

Keqiu Li and Hong Shen, "Optimal Methods for Object Placement for Tree Networks and Autonomous Systems," International Journal of High Performance Computing and Networking, Vol.3, No.5, 2004.

X. Defago, A. Schiper, and P. Urban, "Total Order Broadcast and Multicast Algorithms: Taxonomy and Survey," ACM Computing Surveys, Vol.36, No.4, pp.372-421, Dec. 2004.

X. Defago and A. Schiper, "Semi-passive Replication and Lazy Consensus," Journal of Parallel and Distributed Systems, Elsevier, Vol.64, No.12, pp.1380-1398, Dec. 2004.

A. Miyaji and K. Umeda, "Efficient Group Signature Scheme based on a Modified Nyberg-Rueppel signature," IPSJ Trans, vol. 46, No.8, pp.1889-1902, 2005.

A. Waseda, M. Soshi and A. Miyaji, "Quantum Coin Flipping Protocol Using n-dimensional Quantum States," IPSJ Trans, vol. 46, No.8, pp.1903-1911, 2005.

Y. Sakabe, M. Soshi, and M. Miyaji, "Java Obfuscation - Approaches to Construct Tamper-Resistant Object-Oriented Programs," IPSJ Trans.,vol. 46, No.8, pp.2107-2119, 2005.

Keqiu Li and H. Shen, "Coordinated En-Route Multimedia Object Caching in Transcoding Proxies for Tree Networks," ACM Transactions on Multimedia Computing, Communications and Applications (TOMCAPP), Vol. 1, No. 3, pp.289-314, 2005.

Keqiu Li, H. Shen, F. Chin, and S. Zheng, "Optimal Methods for Coordinated En-Route Web Caching for Tree Networks", ACM Transactions on Internet Technology (TOIT), Vol. 5, No. 3, pp. 480-507, 2005.

Keqiu Li and H. Shen, "Optimal Methods for Proxy Placement in Coordinated En-Route Web Caching," IEICE Trans. on Communications, Vol. E88-B, No. 4, pp. 1458-1466, 2005.

Keqiu Li and H. Shen, "Optimal Methods for Object Placement in En-Route Web Caching for Tree Networks and Autonomous Systems," International Journal of High Performance Computing and Networking (IJHPCN), Vol. 4, No. 5, 2005.

Haibin Kan and Hong Shen, "A Relation Between the Characteristic Generators of a Linear Code and Its Dual," IEEE Transactions on Information Theory, Vol. 51, No. 3, pp. 1199-1202, 2005.

Haibin Kan and Hong Shen, "A Counterexample for the Conjecture on the Minimal Delay of Orthogonal Designs with Maximal Rates," IEEE Transactions on Information Theory, Vol. 51, No. 1, pp. 355-359, 2005.

Gui Xie and Hong Shen, "Highly Scalable, Low-Complexity Image Coding Using Zeroblocks of Wavelet Coefficients," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, No. 6, pp. 762-770, 2005.

Zonghua Zhang and Hong Shen, "Application of Online-training SVMs for Real-time Intrusion Detection with Different Considerations," Computer Communications, Vol.28, No.12, pp.1428-1442, 2005.

Haibin Kan and Hong Shen, "Trellis Properties of Product codes," IEICE Transactions on Fundamentals, Vol. E88-A, No. 1, 2005.

Hui Tian and Hong Shen, "Multicast Based Inference for Topology and Network-Internal Loss Performance from End-to-end Measurements," accepted by Computer Communications, Dec. 2005.

Hui Tian and Hong Shen, "An improved algorithm of multicast topology inference from end-to-end measurements," accepted by International Journal of Communication Systems, 2005.

Hui Tian, Hong Shen and Teruo Matsuzawa, "Energy-Efficient Topologies and Routing for Wireless Sensor Networks", GESTS International Transaction on Computer Science and Engineering, No.1, Vol.8, pp. 79-89, 2005.

Hui Tian, Hong Shen, and Teruo Matsuzawa, "Random Walk Routing for Wireless Sensor Networks," International Journal of Computer Science and Network Security, accepted, 2005.

Ke Deng, Hong Shen, and Hui Tian, "Self projecting time series forecast: an online stock trend forecast system," accepted by International Journal of Computational Science and Engineering, 2005.

W. Qu, H. Shen, and J. Sum, "Stochastic Analysis on Mobile Agent-Based E-Shopping," International Journal of Electronic Business, Vol.3, No.3-4, 2005.

Wenyu Qu, Hong Shen, and John Sum, "New Analysis on Mobile Agents Based," Network Routing. Applied Soft Computing Journal (ASOC), Vol. 6, No. 1, pp. 108-118, 2005.

Stanley P. Y. Fung, Francis Y. L. Chin, and Hong Shen, "Online Scheduling of Unit Jobs with Bounded Importance Eatio," International Journal of Foundations of Computer Science, Vol. 16, No. 3, pp. 581-598, 2005.

Qiangfeng Zhang, Francis Y. L. Chin, and Hong Shen, "Minimum Parent-Offspring Recombination Haplotype Inference in Pedigrees," Transactions on Computational Systems Biology, Vol. 2, pp. 100-112, 2005.

Y. Kozaki-Yamaguchi, N. Suzuki, Y. Fujita, H. Yoshimasu, M. Akagi, and T. Amagasa, "Perception of hypernasality and its physical correlates," Oral Science International, Vol.2, No.1, pp.21-35, 2005.

T. Saitou, M. Unoki, and M. Akagi, "Development of an F0 Control Model Based on F0 Dynamic Characteristics for Singing-voice Synthesis," Speech Communication 46, pp.405-417, 2005.

J. Dang, M. Akagi, and K. Honda, "Communication between Speech Production and Perception within the Brain - Observation and simulation," J. Comp. Sci. & Tech., Vol.21, No.1, pp.95-105, 2006.

J. Li and M. Akagi, "A Noise Reduction System Based on Hybrid Noise Estimation Technique and Post-filtering in Arbitrary Noise Environments," Speech Communication, 48, pp.111-126, 2006.

B. Aronov, T. Asano, N. Katoh, K. Mehlhorn, and T. Tokuyama, "Polyline Fitting of Planar Points under Min-sum Criterion," to appear in International Journal on Computational Geometry and Applications.

T. Asano, P. Evans, R. Uehara, and G. Valiente, "Site Consistency in Phylogenetic Networks with Recombination," In Iliopoulos, C.S., Park, K., Steinh ¨ ofel, K., (eds.): Algorithmics in Bioinformatics. Volume 6 of Texts in Algorithmics. College Publications, pp.15-26, 2006.

Boris Aronov, Tetsuo Asano, Yosuke Kikuchi, Subhas C. Nandy, Shinji Sasahara, and Takeaki Uno, "A Generalization of Magic Squares with Applications to Digital Halftoning," to appear in Theory of Computing System.

S. Sasahara and T. Asano, "New Dispersed-dot Halftoning Technique by Elimination of Unstable Pixels for Electrophotography," Journal of Electronic Imaging, pp.023006-1-9, 2005.

T. Asano, M. de Berg, O. Cheong, H. Everett, H. Haverkort, N. Katoh, and A. Wolff, "Optimal Spanners for Axis-Aligned Buildings," Computational Geometry: Theory and Applications, Vol.30, No.1, pp.59-77, 2005.

国際会議

Takashi Matsunaka, Atsuko Miyaji, and Yuuki Takano, "Success probability in χ^2-attacks," Applied Cryptography and Network Security - ACNS 2004, LNCS 3089, pp.310-325, June 2004.

H. Mamiya, H. Morimoto, and A. Miyaji, "Efficient Countermeasures against RPA," DPA, and SPA", CHES 2004, LNCS 3156, pp.343-356, 2004.

T. Terada, M.Soshi, and A. Miyaji, "A New Pushback Mechanism Resistant to DDoS Attacks," 2004 International Symposium on Information Theory and its Applications - Proceedings of ISITA2004, June 2004.

Atsuko Miyaji and Kozue Umeda, "A Fully-Functional group signature scheme over only known-order group," Applied Cryptography and Network Security - ACNS 2004, LNCS 3089, pp.164-179, June 2004.

Hui Tian and Hong Shen, "Analysis on Binary Loss Tree Classification with Hop Count for Multicast Topology Discovery," 2004 IEEE Consumer Communications and Networking Conference (CCNC 2004), Las Vegas, USA, CD-Rom, Jan. 2004.

Haibin Kan and Hong Shen, and Hong Zhu, "The Closest Vector Problem on Some Lattices," 2nd International Workshop on Grid and Coordinated Computing, Shanghai, China, Dec. 2003.

Zonghua Zhang and Hong Shen, "Online Training of SVMs for Real-time Intrusion Detection," 18th International Conference on Advanced Information Networking and Applications (AINA 2004), 2004.

Keqiu Li and Hong Shen, "Transcoding Proxy Placement in En-Route Web Caching," 2nd Annual Conference on Communication Networks and Services Research (CNSR 2004), pp.276-285, 2004.

Keqiu Li and Hong Shen, "Coordinated En-Route Web Caching in Transcoding Proxies," LNCS 3007 (APWeb 2004), pp.772-781, 2004.

Zonghua Zhang and Hong Shen, "Suppressing False Alarms of Intrusion Detection Using Improved Text Categorization Method," 2004 IEEE International Conference on e-Technology, e-Commerce, and e-Services (EEE 04), pp.163-166, 2004.

Keqiu Li and Hong Shen, "Optimal Placement of Web Proxies for Tree Networks," 2004 IEEE International Conference on e-Technology, e-Commerce, and e-Services (EEE 04), pp.479-486, 2004.

Fei Li, Shile Zhang, Xin Wang,Xiangyang Xue, and Hong Shen, "Vote-Based Clustering Algorithm in Mobile Ad Hoc Networks," LNCS 3090 (ICOIN 2004), pp.13-23, 2004.

Wenyu Qu and Hong Shen, "Some Analysis on Mobile-Agent Based Network Routing," 7th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 2004), pp.2-17, 2004.

Keqiu Li and Hong Shen, "Proxy Placement in Coordinated En-Route Transcoding Caching for Tree Networks," 7th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 2004), pp.226-231, 2004.

Hui Tian and Hong Shen, "Multicast-Based Inference of Network-Internal Loss Performance," 7th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 2004), pp.288-293, 2004.

Hui Tian and Hong Shen, "Mobile Agents Based Topology Discovery Algorithms and Modelling," 7th International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN 2004), pp.502-507, 2004.

Gui Xie and Hong Shen, "A Highly Scalable SPECK Image Coder," IEEE Int. Conf. on Image Processing (ICIP 2004), CD-Rom, Oct. 2004.

Zonghua Zhang and Hong Shen, "Caputure the Drifting of Normal Behavior Traces for Adaptive Intrusion Detection Using Modified SVMs," 3rd International Conference on Machine Learning and Cybernetics (ICMLC2004), pp.3046-3051, Aug. 2004.

Keqiu Li and Hong Shen, "Cache Design for Transcoding Proxy Caching," IFIP International Conference on Network and Parallel Computing 2004 (NPC04), pp.187-194, Oct. 2004.

Keqiu Li and Hong Shen, "An Improved GreedyDual* Cache Document Replacement Algorithm," IEEE/WIC/ACM International Conference on Web Intelligence (WI 2004), pp.457-460, Sept. 2004.

Xiaohong Jiang, Hong Shen, and Susumu Horiguchi, "Performance Analysis of A Novel All-optical Photonic Switch," 7th International Symposium on Contemporary Photonics Technology (CPT2004) , pp.71-72, Jan. 2004.

Xiaohong Jiang, Pin-Han Ho, Hong Shen, and Susumu Horiguchi, "Fault Tolerance Analysis of Optical Switching Systems Built on the Vertical Stacking of Banyan Network," 2004 IEEE Workshop on High Performance Switching and Routing (HPRS 2004), Phoenix, USA , pp.360-364, 2004.

Chao Peng and Hong Shen, "A Storage-aware Scheduling Scheme for VOD," The 3rd International Conference on Grid and Cooperative Computing (GCC'04), Wuhan China, Oct. 2004.

Chao Peng and Hong Shen, "Storage-aware Harmonic Broadcasting Protocol for Video-on-Demand," 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 04), Singapore, Dec. 2004.

Keqiu Li and Hong Shen, "Dynamically Selecting Distribution Strategies for Web Documents According to Access Pattern," 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 04), Singapore, Dec. 2004.

W. Qu and H. Shen, "Analysis of Mobile Agents' Fault-Tolerant Behavior," 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 04), Singapore, Dec, 2004.

Wenyu Qu and Hong Shen, "Mobile Agent-Based Execution Modelling," 4th International Conference on Hybrid Intelligent Systems (HIS'04), Kitakyushu, Japan, Dec. 2004.

Wenyu Qu and Hong Shen, "Behavior Modelling of Mobile Agents' Fault-Tolerant Execution," IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'04), Beijing, China, pp.377-380, Sept. 2004.

W. Qu, H. Shen, and J. Sum, "Further Analysis on the Application of Mobile Agents in Network Routing," International Conference on E-Business and Telecommunication Networks (ICETE'04), Aug. 2004.

Y. Sang and H. Shen, "Novel Impostors Detection in Keystroke Dynamics by Support Vector Machine," 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'04), Singapore, 2004.

Hui Tian and Hong Shen, "Lossy Link Identification for Multicast Network," 5th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'04), Dec. 2004.

Yuanyuan Zhang, Yasushi Inoguchi, and Hong Shen, "A Dynamic Task Scheduling Algorithm for Grid Computing System," 2nd International Symposium on Parallel and Distributed Processing and Applications, pp.578-583, Dec. 2004.

Yuanyuan Zhang and Yasushi Inoguchi, "Influence of Performance Prediction Inaccuracy on Task Scheduling in Grid Environment," The Seventh Asia Pacific Web Conference, Mar. 2005.

K. Satou, Y. Nakajima, S. Tsuji, X. Defago and A. Konagaya, "An Integrated System for Distributed Bioinformatics Environment on Grids," Intl. Workshop on Life Science Grid (LSGRID2004), pp.5-13, May 2004.

X. Defago, "Semi-passive Replication and the Eventual Leadership (invited paper)," Workshop on Dependable Distributed Data Management (WDDDM), pp.13-18, Oct. 2004.

R. Yared, X. Defago, and T. Katayama, "Fault-tolerant group membership protocols using physical robot messengers," 19th IEEE Intl. Conf. on Advanced Information Networking and Applications (AINA), Mar. 2005.

Chun-Fang Huang and Masato Akagi, "A Multi-layer Fuzzy Logical Model for Emotional Speech Perception, " Trans. Tech. Comm. Psychol. Physiol. Acoust., The Acoustical Society of Japan, Vol.34, No.8, H-2004-95, pp.547-552, Kanazawa, Oct. 2004.

Chun-Fang Huang and Masato Akagi, "A perceptual model of emotional speech build by fuzzy logic," ASJ'2004 Fall Metting, pp.287-289, Okinawa, Sep. 2004.

Masaaki Shirase and Yasushi Hibino, "An architecture for Elliptic Curve Cryptograph Computation," Workshop on Architectural Support and Anti-virus (WASSA), Held in cooperation with ASPLOS XI, Oct, 2004.

A. Ben Hassine, X. Defago, and T. B. Ho, "Agent-based Approach to Dynamic Meeting Scheduling Problems," 3rd ACM Intl. Joint Conf. on Autonomous Agents and Multi Agent Systems (AAMAS), Vol.3, pp.1130-1137, July 2004.

A. Ben Hassine, T. Ito and T. B. Ho, "Scheduling Meetings with Distributed Local Consistency Reinforcement," 17th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE 2004), Ottawa, Canada, pp.679-688, 2004.

A. Ben Hassine, K. Ghedira and T. B. Ho, "New Distributed Filtering-Consistency Approach to General Networks," 17th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE 2004), Ottawa, Canada, pp.708-717, 2004.

A. Ben Hassine and T. B. Ho, "DRAC++ for Distributed Restricted Path Consistency," Japan-Tunisia Workshop on Computer Systems and Information Technology (JT-CSIT04), Tokyo 2004.

A. Idrissi and A. Ben Hassine, "Circuit Consistencies," 8th Pacific Rim International Conference on Artificial Intelligence, Auckland, NewZealand 2004, pp. 124-133, 2004.

A. Ben Hassine and T. B. Ho, "Nouvelle Approche Generique pour le Renforcement Distribue de la Consistance de Chemin Restreint," the Scientific French-speaking Workshops (JSF'04), Tokyo, Nov. 2004.

A. Ben Hassine and T. B. Ho, "Restricted Path Consistency Enforcement for any Constraint Network," Joint Workshop of Vietnamese Society of AI, SIGKBS-JSAI, ICS-IPSJ and IEICE-SIGAI on Active Mining AM'04, (IEICE Technical Report Vol.104 No.485), Hanoi-Vietnam, Dec. 2004.

K. Tajima and Y. Fukui, "Answering XPath Queries over Networks by Sending Minimal Views," 30th International Conference on Very Large Data Bases, pp. 48-59, 2004.

A. Waseda, M. Soshi, and A. Miyaji, "*n*-state Quantum Coin Flipping Protocol," International Conference on Information Technology- ITCC2005, Vol. II, pp.776-777, 2005.

H. Mamiya and A. Miyaji, "Fixed-Hamming-Weight Representation for Indistinguishable Addition Formulae," ACNS 2005.

A. Miyaji and Y. Takano, "On the Success Probability of A2-attack on RC6," ACISP 2005, LNCS 3089, pp.310-325, 2005.

Atsuko Miyaji, "Privacy Rights in the Digital Age Technological, -How to Protect Privacy Right by the technology of Information Security-," International Forum on Privacy Rights in the Digital Age, Korean National Commission for UNESCO, Sept. 2005.

A. Miyaji, "On public-key Broadcast Encryption," CSEC2005-29, pp.31-38, 2005.

Toshiyuki Miyachi, Ken-ichi Chinen, and Yoichi Shinoda, "Automatic Configuration and Execution of Internet Experiments on an Actual Node-based Testbed," Tridentcom 2005, Trento, Italy, ISBN 0-7695-2219-X, pp.274-282, Feb. 2005.

A. Miyaji, "ID-Based encryption scheme with a hierarchical structure and its application," Symposium on Cryptography and Information Security, SCIS2006-3A1-4, Jan. 2006.

Ken-ichi Chinen, Toshiyuki Miyachi, and Yoichi Shinoda, "A Rendezvous in Network Experiment - Case Study of Kuroyuri," TridentCom 2006, Barcelona, Spain, ISBN 1-4244-0106-2, Mar. 2006.

Keqiu Li, Hong Shen, and Francis Y. L. Chin, "Cooperative Determination on Cache Replacement Candidates for Transcoding Proxy Caching," LNCS 3619 (Proc. of ICCNMC 2005), pp.178-187, 2005 (Best paper award).

Keqiu Li, H. Shen, Francis Y. L Chin, and Liusheng Huang, "Multimedia Object Placement Solutions for Hybrid Transparent Data Replication," The IEEE Global Telecommunications Conference (GLOBECOM 2005), St. Louis, USA, Nov. 2005.

Hui Tian and Hong Shen, "Discover Multicast Network Internal Characteristics Based on Hamming Distance," 2005 IEEE International Conference on Communications (ICC'05,), Seoul, Korea, CD-ROM, May 2005.

Hui Tian and Hong Shen, "An optimal coverage scheme for wireless sensor network," 2005 IEEE International Conference on Networks (ICN'05), Reunion Island, France, pp. 722-730, April 2005.

Hui Tian and Hong Shen, "Hamming distance and hop count based classification for multicast network topology inference," IEEE 19th International Conf. on Advanced Information Networking and Applications (AINA'05), Taiwan, pp. 267-272, March 2005.

Zonghua Zhang and Hong Shen, "Constructing Multi-Layer Boundary to Defend Against Intrusive Anomalies: An Autonomic Detection Coordinator," Int'l Conf. on Dependable Systems and Networks (DSN2005), Yokohama, Japan, June 2005.

Z. Zhang and H. Shen, "Dynamic Combination of Multiple Host-based Anomaly Detectors with Broader Detection Coverage and Less False Alerts," IEEE Int'l Conf. on Networking (ICN'05), Reunion Island, France, pp.989-996, Apr. 2005.

Yawen Chen and Hong Shen, "An Improved Scheme of Wavelength Assignment for Parallel FFT Communication Pattern on a Class of Regular Optical Networks," LNCS 3779 (Proc. of 2005 IFIP Int. Conf. on Networks and Parallel Computing), Beijing, pp.189-196, Dec. 2005.

Wenyu Qu and Hong Shen, "Theoretical Analysis on A Traffic-Based Routing Algorithm of Mobile Agents," IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'05), France, pp.520-526, Sep. 2005.

Keqiu Li, Keishi Tajima, and Hong Shen, "Cache Replacement for Transcoding Proxy Caching," IEEE/WIC/ACM Int'l Conf. on Web Intellig. (WI'05), France, pp.500-507, Sep. 2005.

Haibo Zhang, Hong Shen, and Haibin Kan, "Reliability-Latency Tradeoffs for Data Gathering in Random-Access Wireless Sensor Networks," LNCS 3619 (Proc. GCC 2005), pp. 701-712, 2005.

Wenyu Qu, Hong Shen, Yingwei Jin, "Distribution of Mobile Agents in Vulnerable Networks", Lecture Notes in Computer Science 3619 (Proc. GCC 2005), 2005, p. 894-905.

W. Chan, F. Y. L. Chin, Y. Zhang, H. Zhu, H. Shen, and P. W. H. Wong, "Off-Line Algorithms for Minimizing Total Flow Time in Broadcast Scheduling," LNCS 3595 (Proc. COCOON 2005), pp.318-328, 2005.

Keqiu Li, Hong Shen, and Francis Y. L. Chin, "Placement Solutions for Multiple Versions of A Multimedia Object," 8th IEEE Int. Symp. on Object-Oriented Real-Time Distributed Computing (ISORC2005), Seattle, USA, pp. 224-231, May 2005.

Yingpeng Sang, Hong Shen, and Zonghua Zhang, "An Efficient Protocol for the Problem of Secure Two-party Vector Dominance," 6th Int'l Conf. on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2005), Dalian, pp. 488-492, Dec. 2005.

Xavier Défago, Péter Urbán, Naohiro Hayashibara, and Takuya Katayama, "Definition and Specification of Accrual Failure Detectors," Intl. Conf. on Dependable Systems and Networks (DSN), pp. 206-215, 2005.

Koji Ohashi and Mineo Kaneko, "Statistical Scheduling Length Analysis In Asynchronous Datapath Synthesis," IEEE International Symposium on Circuits and Systems, pp.700-703, May 2005.

Koji Ohashi and Mineo Kaneko, "Statistical Analysis Driven Synthesis of Asynchronous Systems," International Conference on Computer Design, pp.200-205, Oct. 2005.

Takayuki Obata and Mineo Kaneko, "Control Signal Skew Scheduling in RT Level Datapath Synthesis," IEEE International Midwest Symposium on Circuits and Systems, CD-ROM ISBN:0-7803-9198-5, Aug. 2005.

Mineo Kaneko, "Sequence Triple: A Finite Solution Space for Repeated Placement," IEEE International Midwest Symposium on Circuits and Systems, CD-ROM ISBN:0-7803-9198-5, Aug. 2005.

M. Unoki, M. Toi, and M. Akagi, "Development of the MTF-based Speech Dereverberation Method using Adaptive Time-frequency Division," Forum Acousticum 2005, pp.51-56, 2005.

J. Li, X. Lu and M. Akagi, "Noise Reduction based on Microphone Array and Post-filtering for Robust Speech Recognition in Car Environments," Workshop DSPinCar2005, S2-9, 2005.

C. F. Huang and M. Akagi, "A Multi-Layer Fuzzy Logical Model for Emotional Speech Perception," EuroSpeech2005, Lisbon, Portugal, pp.417-420, 2005.

M. Unoki, M. Kubo, A. Haniu, and M. Akagi, "A Model for Selective Segregation of a Target Instrument Sound from the Mixed Sound of Various Instruments," EuroSpeech2005, Lisbon, Portugal, pp.2097-2100, 2005.

J. Li and M. Akagi, "A Hybrid Microphone Array Post-filter in a Diffuse Noise Field," EuroSpeech2005, Lisbon, Portugal, pp.2313-2316, 2005.

J. Li and M. Akagi, "Theoretical Analysis of Microphone Arrays with Postfiltering for Coherent and Incoherent Noise Suppression in Noisy Environments," IWAENC2005, Eindhoven, The Netherlands, pp.85-88, 2005.

J. Nakanishi, M. Unoki and M. Akagi, "Effect of ITD and Component Frequencies on Perception of Alarm Signals in Noisy Environments," NCSP2006, pp.37-40, 2006.

T. T. Vu, M. Unoki, and M. Akagi, "A Study on an LPC-based Restoration Model for Improving the Voice-quality of Bone-conducted Speech," NCSP2006, pp.110-113, 2006.

H. Nishimoto and M. Akagi, "Effects of complicated vocal tract shapes on vocal tract transfer functions," NCSP2006, pp.114-1172006.

Y. Takeyama, M. Unoki, M. Akagi, and A. Kaminuma, "Synthesis of Mimic Speech Sounds Uttered in Noisy Car Environments," NCSP2006, pp.118-121, 2006.

X. Lu, M. Unoki, and M. Akagi, "MTF-based Sub-band Power Envelope Restoration in Reverberant Environment for Robust Speech Recognition," NCSP2006, pp.162-165, 2006.

J. Dang, J. Wei, T. Suzuki, and P. Perrier, "Investigation and Modeling of Coarticulation during Speech," Interspeech2005, Lisbon, Portugal, pp. 1025-1028, 2005.

J. Wei, X. Lu, and J. Dang, "Parameter Optimization for a Coarticulation Model based on Observation and Simulation," International Symposium of Frontiers in Speech and Hearing Research, pp.49-54, 2006.

T. Asano, F. Rossello and G. Valiente, "Template Matrices for Perfect Phylogeny Haplotyping and Site Consistency," RECOMB2006, 2006

T. Asano, S. Choe, S. Hashima, Y. Kikuchi, and S.-C. Sung, "Distributing Distinct Integers Uniformly over a Square Matrix with Application to Digital Halftoning," Invited Talk at 7th Hellenic European Conference on Computer Mathematics and its Applications, Athens, Greece, Sept. 2005.

Xuefeng Liang, Kazunori Kotani, and Tetsuo Asano, "Automatically Choosing Appropriately-Sized Structuring Elements to Eliminate Useless Components in Fingerprint Image," Visual Communications and Image Processing 2005, Beijing, edited by Shipeng Li, Fernando Pereira, Heung-Yeung Shum, Andrew G. Tescher, Proc. Of SPIE Vol.5960, pp.284-293, 2005.

T. Asano, "Computational Geometric and Combinatorial Approaches to Digital Halftoning," Prenaru Talk at International Conference on Computational Science and Its Applications, Singapore, May 2005.

S. Teramoto, T. Asano, B. Doerr, and N. Katoh, "Inserting Points Uniformly at Every Instance," 2005 Korea Japan Joint Workshop on Algorithms and Computation, Seoul, Korea, pp.3-9, 2005.

E. Chiba, T. Asano, T. Miura, N. Katoh, and I. Mitsuka, "Modeling of Transportation Systems Using Crash Probability," 2005 Korea Japan Joint Workshop on Algorithms and Computation, pp.142-149, Seoul, Korea, 2005.

その他（国内会議等）

宮地充子, "双線型写像の公開鍵暗号への応用に関して," 符号と暗号の代数的数理, 京都大学数理解析研講究録 1420, pp.117-127, 2005.

早稲田篤志, 双紙正和, 宮地充子, "*n*状態量子コイン投げプロトコル," IEICE Japan Tech. Rep., ISEC2004-10, pp.65-68, May 2004.

佐々木賢, 早稲田篤志, 双紙正和, 宮地充子, "量子秘密分散に関する検討," IEICE Japan Tech. Rep., IT2004-71, ISEC2004-127, WBS2004-186, pp.7-11, Mar. 2005.

森正行, 双紙正和, 宮地充子, "モバイルエージェント・セキュリティに関する一考察," 2005-CSEC-28, pp.123-128, Mar. 2005.

白勢政明,日比野靖, "CMOSトランスファーゲートによる三値論理回路とその構成法," 多値論理とその応用研究会, 2005.

X. H. Phan and M. L. Nguyen, "Flexible Conditional Random Fields Toolkits," http://www.jaist.ac.jp/~hieuxuan/flexcrfs/flexcrfs.html

宮地充子, "（招待講演）ユビキタス社会と情報セキュリティ,"サイバネティック・フレキシブル・オートメーション (CFA) 研究分科会第20 回研究例会, 2005.

宮地充子, 近澤武, 竜田敏男, 大塚玲, 安田幹, "（解説）情報セキュリティの標準化動向について－ ISO/IEC JTC1/SC27/WG2 2005 年 月ウィーン会議報告－," 電子情報通信学会, 信学技報ISEC 2005-7, 2005.

寺田 剛陽, 双紙 正和, 宮地 充子, "変動マーキング確率を用いるIPトレースバックの効果," CSS2005 (Computer Security Symposium 2005), pp.253-258, Oct. 2005.

早稲田篤志, 双紙正和, 宮地充子, "n次元量子状態を使用した量子コイン投げプロトコル," 情報処理学会論文誌,Vol.46, No.8, pp.1903-1911, 2005.

宮地充子, "双線型写像の公開鍵暗号への応用に関して," 符号と暗号の代数的数理, 京都大学数理解析研講究録, 1420, pp.117-127, 2005.

早稲田篤志, 双紙正和, 宮地充子, "MSPを使った量子複数秘密分散に関する考察,"IEICE Japan Tech. Rep., ISEC2005-119, pp.53-60, Dec. 2005.

宮地充子, 清宮健, "Address-bit DPAに強力なBRIPアルゴリズムの改良,"IEICE Japan Tech. Rep., ISEC2005-118, pp.47-52, Dec. 2005.

宮地充子, "双線形写像に基づく暗号に適した（超）楕円曲線の構成,"「代数幾何・数論及び符号・暗号」研究集会報告書, 東京大学大学院数理科学研究科, Jan, 2006.

樋上智彦, 宮地充子, "RC6のX二乗攻撃の効率化へのアプローチについて," Symposium on Cryptography and Information Security, SCIS2006-3A1-4, Jan. 2006.

寺家谷純, 宮地充子, "階層的IDベース署名の構築にむけて," ISEC, Mar, 2006.

清宮健, 宮地充子, "効率的なDPAとSPAに強力な予備演算テーブルを用いたスカラー倍算アルゴリズム," ISEC, Mar. 2006.

田中大嗣, 宮地充子, "効率的な削除機能を持つグループ署名,"CSEC, Mar. 2006.

服部太郎, 双紙正和, 宮地充子, "動的解析に対し耐タンパ性を持つ難読化手法の提案," CSEC, Mar. 2006.

宮地利幸, 知念賢一, 篠田陽一, "SpringOS/VM: 大規模ネットワークテストベッドにおける仮想機械運用技術," 情報処理学会研究報告書,2005-OS-99, pp.105-112, May 2005, ISSN 0919-6072.

三輪信介, 宮地利幸, 大野浩之, "不正アクセス等再現実験環境の統合実験," マルチメディア, 分散, 協調とモバイル (DICOMO2005)シンポジウム論文集, pp.393-396, ISSN1344-0640, 情報処理学会, Jul. 2005.

白勢政明, 日比野靖, "標数3の体でのXTR," 信学技法, Vol.105, No.51, (ISEC2005-3), May 2005.

白勢政明, 日比野靖, "XTRに適したディジタル署名方式,"信学技法, Vol. 105, No.395, (ISEC2005-96), Nov. 2005.

Koji Ohashi and Mineo Kaneko, "Simultaneous Scheduling and Binding for Asynchronous System with Statistical Makespan Analysis," 第18回回路とシステム軽井沢ワークショップ論文集 pp. 587-592, Apr. 2005.

Takayuki Obata and Mineo Kaneko, "Control Signal Skew Scheduling for RT Level Datapaths," 第18回回路とシステム軽井沢ワークショップ論文集, pp.521-526, Apr. 2005.

Mineo Kaneko, "Statistical Properties and Subclasses of Sequence Triple Code Space for Repeated Placement," IEICE Techinical Report, CAS2005-66, CST2005-35, pp.31-36, Nov. 2005.

Mineo Kaneko, "Minimal Set of Essential Lietime Overlaps for Exploring 3D Schedule," IEICE Techinical Report, VLD2005-64, ICD2005-159, DC2005-41, pp.19-24, Dec. 2005.

Koji Ohashi and Mineo Kaneko, "Resource Sharing in Dual-Rail Two-Phase Asynchronous Datapath Synthesis," IEICE Techinical Report, CAS2005-93, pp.37-42, Jan. 2006.

Takayuki Obata and Mineo Kaneko, "Simultaneous Control-step and Skew Assignment for Control Signals in RT-Level Datapath Synthesis," IEICE Techinical Report, CAS2005-92, pp.31-36, Jan. 2006.

小畑貴之, 金子峰雄, 平石邦彦, "温度並列SAのシーケンスペアによるパッキング問題への適用," 電子情報通信学会全国大会, Mar. 2006.

K. Maki and M. Akagi, "A Computational Model of Cochlear Nucleus Neurons," In Auditory Signal Processing, Springer, pp.84-90, 2005.

K. Ito and M. Akagi, "Study on Improving Regularity of Neural Phase Locking in Single Neurons of AVCN via a Computational Model," In Auditory Signal Processing, Springer, pp.91-99, 2005.

C. F. Huang and M. Akagi, "Toward a Rule-based Synthesis of Emotional Speech on Linguistic Description of Perception," Affective Computing and Intelligent Interaction, Springer LNCS 3784, pp. 366-373, 2005.

T. T. Vu, M. Unoki, and M. Akagi, "A Study on Restoration of Bone-conducted Speech with the Lpc-based Model," Int. Sympo. Frontiers in Speech and Hearing Research, pp.67-72, 2006.

X. Lu, M. Unoki, and M. Akagi, "Sub-band Temporal Envelope Restoration for ASR in Reverberation Environment," Int. Sympo. Frontiers in Speech and Hearing Research, pp.73-78, 2006.

赤木正人, "表現豊かな音声　―その生成・知覚と音声合成への応用―," 日本音響学会誌, Vol.61, No.6, 346-351, 2005.

鵜木, 木村, 赤木, "変調伝達特性に着目した骨導音声回復法の検討," 音響学会聴覚研究会資料, H-2005-33, 2005.

鵜木, 戸井, 赤木, "変調伝達関数に基づいた残響音声回復法の改良と総合評価," 音響学会聴覚研究会資料, H-2005-55, 2005.

黄, 赤木, "感情知覚モデルを検証するための規則の構築," 電子情報通信学会技術報告, SP2005-39, 2005.

J. Li and M. Akagi, "A Noise Reduction Method based on a Generalized Subtractive Beamformer," Tech. Report of IEICE, EA2005-44, 2005.

齋藤, 鵜木, 赤木, "自然性の高い歌声合成のためのヴィブラート変調周波数の制御法の検討," 電子情報通信学会技術報告, TL2005-10, 2005.

C. F. Huang and M. Akagi, "Rule-Based Speech Morphing for Evaluating Linguistic Descriptions of Emotional Speech Perception," ASJ '2005 Fall Meeting, 1-6-3, 2005.

J. Li and M. Akagi, "A Noise Reduction Method based on a Generalized Subtractive Beamformer," ASJ '2005 Fall Meeting, 2-2-19, 2005.

齋藤, 赤木, 榊原, "声区変換を伴う歌声合成を目的とした音響パラメータ制御法の検討,"平成17年秋季音響学会講演論文, 2-6-10, 2005.

鵜木, 木村, 赤木, "変調伝達関数に着目した骨導音声回復法の検討," 平成17年秋季音響学会講演論文、2-Q-23, 2005.

西本, 赤木, 党, 鈴木, "口腔疾患患者の調音時の補償動作に着目した変形声道モデルによる伝達特性の分析," 平成17年秋季音響学会講演論文, 3-1-15, 2005.

T. T. Vu, M. Unoki, and M. Akagi, "A Method for Restoring Bone-conducted Speech base on LPC Model," ASJ '2006 Spring Meeting, 1-3-3, 2006.

鵜木, Lu, 赤木, "残響にロバストな音声認識のための帯域分割型パワーエンベロープ回復処理の検討," 平成18年春季音響学会講演論文, 1-5-5, 2006.

竹山, 鵜木, 赤木, 神沼, "自動車走行雑音下における車室内発話音声の合成," 平成18年春季音響学会講演論文, 1-Q-18, 2006.

中西, 鵜木, 赤木, "雑音中の報知音知覚における報知音のITD および成分周波数の影響,"平成18年春季音響学会講演論文, 2-3-1, 2006.

田中, Lu, 党, 赤木, "変形聴覚フィードバックにおける摂動量と補正動作の関係について", 平成18年春季音響学会講演論文, 2-3-11, 2006.

J. Li, M. Akagi, and Y. Suzuki, "Two-microphone Noise Reduction with Preserving ITD Cues in Highly Non-stationary Multi-noise-source Environments," ASJ '2006 Spring Meeting, 3-5-10, 2006.

D. Ying, Soong Shi. Y., and J. Dang, "A Robust VAD based upon Noise Eigenspace Projection," Spring Meeting of The Acoustical Society of Japan, pp.147-148, 2006.

錦戸信和, 党建武, "モデルを用いた模擬に基づく発話状態の多意性の分析," 日本音響学会全国大会論文集, pp.261-262, 2006.

平成18年度以降の計画と展望

本拠点では、(1) 電子社会システムに対する形式的定義・検証手法、ソフトウェアモデリング技術の適用によって安心性の高い電子社会モデルを獲得し、(2) それをセキュリティや安心性の保障された情報基盤上に実現する、という方法論によって安心電子社会システムを実現するための拠点形成を行い、研究および人材養成に関して所定の成果を上げてきた。平成 18 年度以降についても、独創的で画期的な研究成果を目指して以下のような研究を行う。研究成果については、これまで通り国際会議や学会論文などで発表を行っていくが、まとまった成果については、JAIST 出版局から Research Monograph Series on COE Program "Verifiable and Evolvable e-Society" の中で順次出版を行うことを計画している。人材養成については、当初の計画にしたがって博士後期課程学生とポスドクの養成を行う。

電子社会のための法令文書の論理表現と推論グループ

主な研究課題は、(a) 自然言語によって書かれた法令文の形式論理への変換、および、(b) その形式論理のための推論システムの設計・構築である。(a) においては、これまで千代田区や富山県の条例を対象にして論理式への変換方法の検討を行ってきた。変換方法は手続き的方法と機械学習を用いる方法の検討を行った。今後は二つの方法について変換の精度やカバー範囲を広げるために研究を進める。(b) においては、法令の変更などの際に重要となる、法令知識ベースの矛盾の検出方式を検討してきたが、今後は、矛盾を修正する論駁推論の研究を併せて進め、法推論システムの構築を行う。

電子社会のための形式推論機構グループ

形式検証のための推論機構について、(a) 推論における証明論的方法と代数的方法の間接な関係があることをいろいろな角度から明らかにしてきた。そのひとつとして、論理における証明の導出と代数における等式の導出は、代数化の概念で明確に関係付けられることを解明した。今後は、この考えを一層進め、代数化によりさまざまな論理的内容を代数的に特徴付ける研究を行う。(b) 人間にとっては自然な古典論理的証明を計算論的意味の明確な構成的論理における証明に変換する方法の研究、特に、自動変換が可能な問題のクラスの明確化と変換機構の研究を行う。

電子社会のための形式検証技術グループ

電子社会の安心性検証のための種々の検証技術を研究する。具体的には、電子社会の基本構成要素であるポリシー、ドメイン、ワークフロー（プロセス）の形式記述と検証を、いくつかの重要な応用分野において展開し、包括的な検証技術を開発する。ポリシーに関しては、(a) オブジェクト指向論理に基づくファイアーウォールのセキュリティポリシーの形式記述と検証、ドメインに関しては、(b) 電子取引ドメインの CafeOBJ や VDM による形式記述と検証、ワークフローに関しては、(c) 組織内ワークフローの規則・法令整合性、ワークフロー管理問題の形式記述と検証を行う。

電子社会のためのモデル化技術グループ

電子社会モデルにアカウンタビリティや進化機構を組み込む研究を行う。アカウンタビリティと進化容易性の実現のためには、法令文とシステム構成要素間の対応関係保持データベース、新旧法令間の整合性判定機構、法令改定のための版管理機構、多様な利害関係者からの質問に答える説明機構、説明機構をシステムに装着するアーキテクチャなどが必要なことが判明し、基本的検討を加えてきた。今後は、事例についての詳細な研究の後に、理論的体系化を行う。

電子社会のための安心基盤技術グループ

安心な電子社会情報システムを実現するための種々の安心基盤技術、(a) 暗号、認証などのセキュリティコア技術、(b) ネットワークや分散システムの安心性技術、(c) ハードウェアや組込みシステムなどの高信頼化技術、などの研究を行ってきた。引き続き、(a) セキュリティシステム故障時の安全・安心性を確保する高度暗号や耐タンパソフトウェア、公開鍵暗号処理ハードウェア、(b) インターネットシミュレータを用いたネットワーク安心性検証や分散システムのためのジェネリックな誤りノード検出モジュールの開発、(c) 組込みソフトウェアのためのモデル検査技術、ハードウェア自動合成、安心ヒューマンインタフェースの研究を行う。

JAIST 21世紀COEプログラム
検証進化可能電子社会　中間報告書

発行　平成18年3月

連絡先　北陸先端科学技術大学院大学
安心電子社会研究センター

〒923-1292 石川県能美市旭台1-1
TEL:0761-51-1975 FAX:0761-51-1149
E-MAIL: coe-trust@jaist.ac.jp
URL: http://www.jaist.ac.jp/jaist-coe