JAIST
21世紀COEシンポジウム2006
検証進化可能電子社会

Programs

2006年3月8日（水）

10:00 - 17:30 **GRP研究員発表会**

2006年3月9日（木）

10:00 **基調講演**

「検証進化可能電子社会」の実現にむけて
片山　卓也（拠点リーダー）

10:45 - 12:15 **セッション1　論理と法推論**

論理における証明論的方法と代数的方法の接点
小野　寛晰（*1）

法律知識の矛盾の発見・解消を行う論理システム
東条　敏（*1）

法律条文の言語処理　島津　明（*1）

13:15 - 15:15 **セッション2　モデル化と検証**

CafeOBJを用いた形式手法―実行可能形式仕様言語による
システム検証―　二木　厚吉（*1）

ビジネスプロセスの安心性検証　平石　邦彦（*1）

モデル化と証明に基づく電子社会の安心性検証
小川　瑞史（*2）

ソフトウェアアカウンタビリティの定義と実現法
落水浩一郎（*1）

15:30 - 17:00 **セッション3　セキュリティとインフラストラクチャー**

電子社会の安心性検証のための情報セキュリティ
宮地　充子（*1）

Fault-tolerant group communication protocols and fault-detection for distributed systems and their application to autonomous mobile systems　Xavier Defago（*1）

インターネットシミュレータによる電子社会の安心性検証
篠田　陽一（*3）

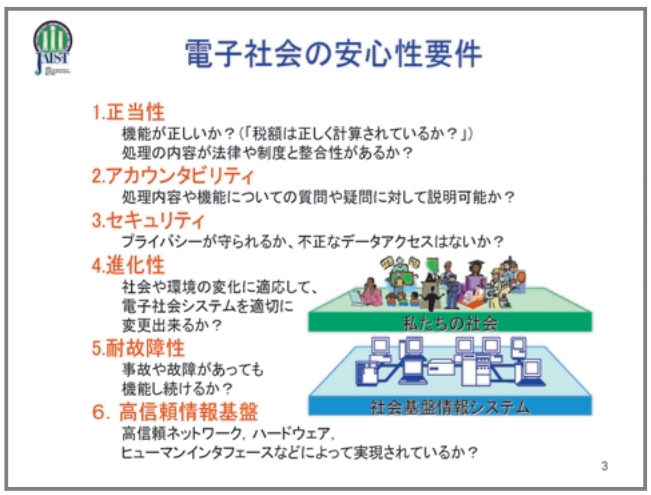
※講演者の所属
*1　北陸先端科学技術大学院大学 情報科学研究科
*2　北陸先端科学技術大学院大学 安心電子社会研究センター
*3　北陸先端科学技術大学院大学 情報科学センター

「検証進化可能電子社会」の実現にむけて

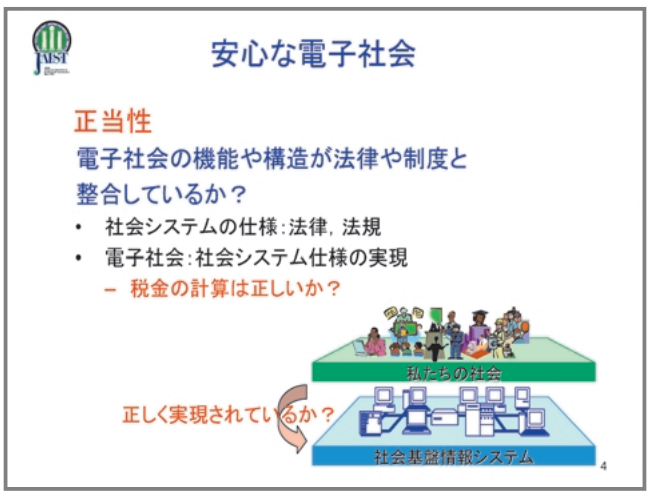
片山　卓也
拠点リーダー

1

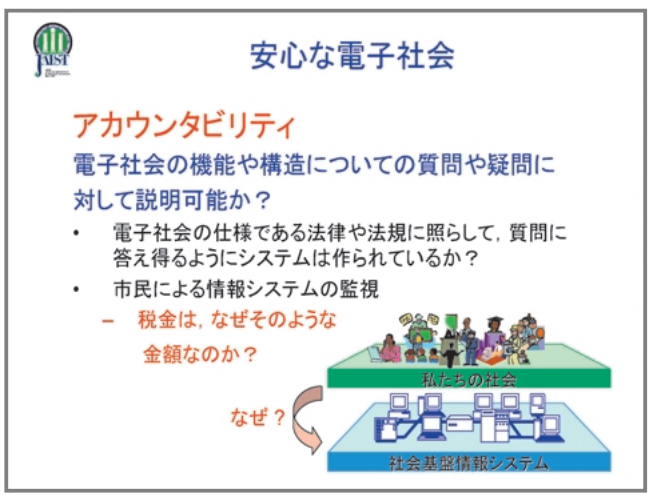
2



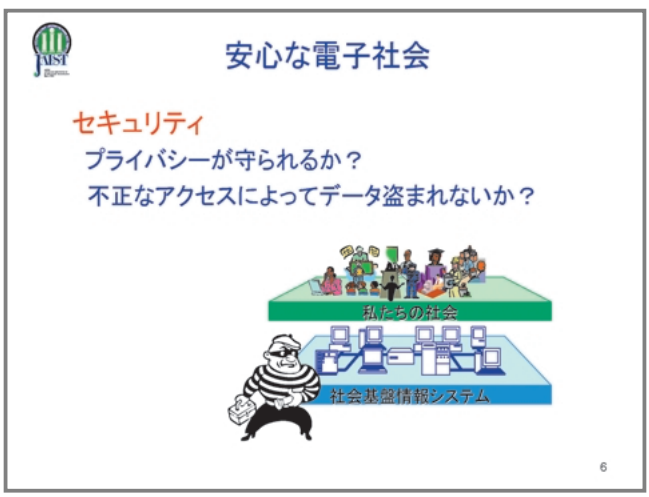
3



4



5



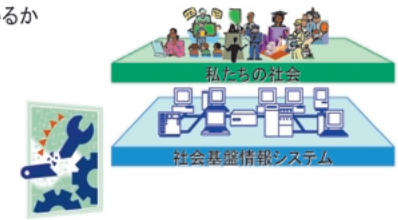
6

安心な電子社会

耐故障性

事故や故障があっても電子社会は機能し続けか？

- どのような形で冗長性や回復のメカニズムが組み込まれているか
- 原子的同報通信や合意形成などの機構は，耐故障になっているか



7

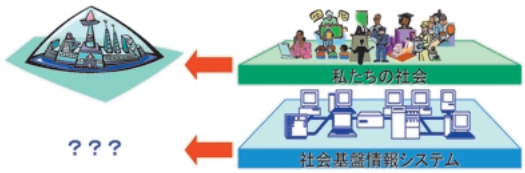
7

安心な電子社会

進化性

社会情勢や環境の変化に適応して、電子社会を適切に変更出来るか？

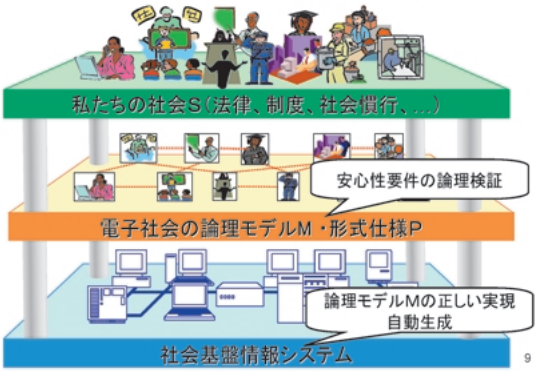
- 進化性がないと社会の停滞を招く



8

8

安心性要件を満たす電子社会の実現法
形式手法＋モデル指向



9

9

「検証進化可能電子社会」

- 「検証進化可能電子社会」
  ―情報科学による安心電子社会の実現―
- 21世紀COEプログラム，H16年度採択（革新的分野）
- 最新の情報科学の成果を利用し，安心な電子社会の構築に寄与する．
- 北陸先端大情報科学研究科を中心にして，次の観点から研究教育を行う．
  - 検証進化可能電子社会の研究
    - 形式論理，ソフトウェア技術，人工知能の立場から
  - 安心電子社会基盤の研究
    - アルゴリズム，ネットワーク，ハードウェア，ヒューマンインタフェースの立場から

10

10

拠点形成の目的―研究―

- 電子社会の検証・進化に関する学問分野の創設
  - 電子社会の形式的仕様記述方法論
  - 安心性要件の論理検証・実現方法論
  - 論理検証方式
  - 電子社会のモデル化とシミュレーション
  - 電子社会の進化機構
  - 電子社会のための基盤情報システム

11

11

拠点形成の目的―人材養成―

- 電子社会の検証・進化技術をもった人材の養成
  - 大学院博士後期課程学生、ポスドクを対象
    - 電子社会、電子政府の設計、検証、進化の中核となる高級技術者の養成
  - 体系的な先端講義カリキュラムによる基本原理・技術の教育
    - 現行の高信頼システム・ソフトウェア、セキュリティ講義群
    - 電子社会検証進化に特化した講義群
  - 電子社会モデリング、検証プロジェクトへの参加による実践的開発技術の養成
    - システム開発能力の評価体制と博士号の授与
  - 30名の博士レベルの研究者・高級技術者を養成

12

12

拠点の革新性

- 電子社会の安心性の確保に厳密な論理的手法を採用
  - 定理証明技術、形式仕様・モデル化技術などの最新の情報科学を適用
  - 電子社会全体のモデル化・仕様化，論理検証
- 電子政府・社会のための「従来の」情報技術
  - データ技術：電子社会の中のデータ
    - Web、ワークフロー、データベース、データマイニング
  - セキュリティ技術：データの保護、保全
    - 暗号、プロトコル検証、インフォーメーションフロー

13

13

検証進化可能電子社会研究
－ 課題，体制，中間成果 －

14

14

「検証進化可能電子社会」研究全体像

15

15

「検証進化可能電子社会」事業推進担当者

16

16

安心電子社会研究センター

- 目的
  - 安心な電子社会を実現するための研究やプロジェクトの企画と推進
  - 安心な電子社会を実現する能力を有する人材を養成する教育プログラムの開発及び実施
  - 国内外の教育研究機関との連携推進
- 組織（平成18年3月現在）
  - センター長
  - 研究員
    - 特任教員　2名
    - 客員教員　2名，客員研究員　1名
    - ポスドク　5名
    - 博士学生研究員　24名
  - 事務員

17

17

国内連携体制

- 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
- インテック・ウェブ・アンド・ゲノム・インフォマティックス（株），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
- 北陸NES（株）
  - 連携内容：形式手法によるプロトコル検証
- NICT
  - 連携内容：インターネットシミュレータとその応用
- 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

18

18

国外連携体制

- AT&T Labs-Research
  - 連携内容：高信頼情報システム構築法
- 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
- 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
- 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
- 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
- デンマーク工科大学
  - 連携内容：形式方法論

19

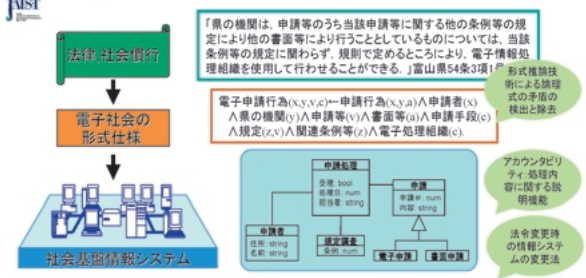
19

「検証進化可能電子社会」中間成果概略

20

20

法推論とモデル化技術

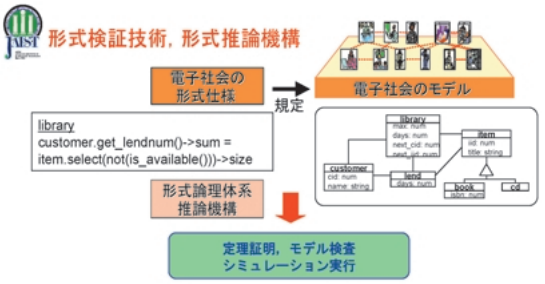


- Law-Defined Information System:「法令文は電子社会情報システムの仕様である」
  - -法律の構造にもとづくシステムの構築と進化，アカウンタビリティ機構の導入
  - -法律全般では，不可能．情報システムとして実現される法令のみを対象
- 研究内容と成果
  - -富山県・千代田区条例，Jaist規則の調査
  - -法令文に適した論理式の決定，法令文=>論理式変換方式
  - -形式推論による法令文論理式データベースからの矛盾の検出・除去アルゴリズム
  - -情報システムへのアカウンタビリティ機構組込み方式，法令変更への対応
- 電子社会情報システム構築の新しい方法論—本COEの提案

21

21

形式検証技術，形式推論機構



- 電子社会情報システムの正しさの検証の基幹技術
  - -電子社会システムが正しさを定理証明，モデル検査技術，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によるオブジェクト論理の実装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は，本COEはわが国最大規模，論理の数学的基礎付けについては，世界的センター

22

22

安心基盤技術

- 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
  - -階層的公開鍵暗号方式
  - -3値論理暗号ハードウェア
  - -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(NICT)によるネットワークセキュリティ・耐故障検証研究

23

23

論理における証明論的方法と代数的方法の接点

小野　寛晰
北陸先端科学技術大学院大学 情報科学研究科

論理における証明論的方法と代数的方法の接点

小野　寛晰

形式的仕様記述体系グループ

1

証明論的方法と代数的方法

1. 論理の証明体系と代数に対する計算体系

- deduction と equational consequence の関係を明らかにする (cf. algebraic specification)

2. cut elimination の代数的意味

1. N. Galatos and HO, Algebraization, parameterized local deduction theorem and interpolation theorem for substructural logics over FL, to appear in Studia Logica 83, 1-32 (2006).
2. F. Belardinelli, P. Jipsen and HO, Algebraic aspects of cut elimination, Studia Logica 77, 209-240 (2004).

2

論理への代数的アプローチ

- 非古典論理の意味論としての代数的構造
- universal algebra や algebraic logic の方法や成果を利用
- さまざまな論理を代数的視点から統一的に理解することを可能にする

証明論的方法は特定の論理についての深い理解をあたえ、代数的方法は多くの論理に共通な性質についての広い知識をあたえる．対象についての多様な側面を知ることにより、その本質に迫ることができる．

3

論理計算と論理の代数化

論理の代数化、等式の計算としての論理計算、抽象代数としてのブール代数

- Boole, De Morgan, Schröder

G. Boole, The Mathematical Analysis of Logic — being an essay towards a calculus of deductive reasoning, 1847

２０世紀における代数的アプローチの展開

- Łukasiewicz, Tarski, Lindenbaum, Rasiowa （ポーランド学派）
- Tarski, Jónsson, Blok, Pigozzi (universal algebra)

4

代数的方法に対する再認識

Gian-Carlo Rota 著 "Indiscrete Thoughts" (1996) より。

"Ever since theoretical computer scientists began to upstage traditional logicians we have watched the resurgence of nonstandard logics. These new logics are feeding problems back to universal algebra, with salutary effects. Whoever believes that the theory of commutative rings is the central chapter of algebra will have to change his tune. The combination of logic and universal algebra will take over."

5

Provability と Deducibility

以下では直観主義論理に対するシーケント計算 **LJ** とハイティング代数のクラス HA を例にとる。

- $\vdash_{LJ} \alpha_1, \ldots, \alpha_m \Rightarrow \beta$ とは、**LJ** でシーケント $\alpha_1, \ldots, \alpha_m \Rightarrow \beta$ が証明される (provable) こと
- $\alpha_1, \ldots, \alpha_m \vdash^*_{LJ} \beta$ とは、$\Rightarrow \alpha_i \ (i = 1, \ldots, m)$ を新たに initial sequents としてつけ加えた体系で $\Rightarrow \beta$ が **LJ** で導出される (deducible) こと

演繹定理

$\Gamma \vdash^*_{LJ} \beta \iff \Gamma \Rightarrow \beta$ is provable in **LJ**.

6

FOLの枠組みでの代数的解釈

シーケント $\alpha_1, \ldots, \alpha_m \Rightarrow \beta$ の provability (論理式 α_i, β と term s_i, t を同一視)

- The inequation $\forall \bar{x}(s_1 \wedge \ldots \wedge s_m \leq t)$ follows from the axioms for HA in FOL

β の $\alpha_1, \ldots, \alpha_m$ からの deducibility

- The universal Horn sentence (quasi-equation) $\forall \bar{x}((s_1 = 1 \text{ and } \ldots \text{ and } s_m = 1) \text{ imply } t = 1)$ follows from the axioms for HA in FOL

演繹定理 によりこれら二つの条件が等しい。しかし一般の substructural logic では演繹定理は成立しない

7

等式計算の体系 1

HA のように、その公理がすべて equation で表されるような代数のクラスを equational class (または variety) という。

対象とする代数のクラスが equational class の場合 quasi-equations の導出可能性は FOL の部分体系である equational calculus で考えれば十分

8

等式計算の体系 2

- $s = s$
- $s = t$ implies $t = s$
- $s = t$ and $t = r$ imply $s = r$
- $s_1 = t_1$ and ... and $s_n = t_n$ imply $f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)$

ここでは Birkhoff の equational logic とは異なり一般的な形での代入の規則は仮定しない。その代わりつぎの仮定をおく

- $u = w$ ただし、$u = w$ が HA のある公理の代入例のとき

9

Equational consequence

$E \vdash_{HA} u = v$ とは、等式の集合 E に属す等式を公理としてつけ加えたときに、等式計算の体系で等式 $u = v$ が導かれること

Algebraization Theorem (の変形)

- $\alpha_1, \ldots, \alpha_m \vdash^*_{LJ} \beta \iff \{\alpha_1 = 1, \ldots, \alpha_m = 1\} \vdash_{HA} \beta = 1$
- $s_1 \leftrightarrow t_1, \ldots, s_n \leftrightarrow t_n \vdash^*_{LJ} u \leftrightarrow v \iff \{s_1 = t_1, \ldots, s_n = t_n\} \vdash_{HA} u = v$
- $(s \leftrightarrow t) = 1 \iff s = t$, α is provably equivalent to $\alpha \leftrightarrow 1$

10

Algebraizability

論理 (deducibility) と equational class (equational consequence) を結ぶ一般的なスキーマ

論理 $\mathbf{L}$ — equational class V (= Mod($\{\varphi = 1 : \varphi \in \mathbf{L}\}$))

- $\alpha_1, \ldots, \alpha_m \vdash^*_L \beta \iff \{s_1 = 1, \ldots, s_m = 1\} \vdash_V t = 1$
- $s_1 \leftrightarrow t_1, \ldots, s_n \leftrightarrow t_n \vdash^*_L u \leftrightarrow v \iff \{s_1 = t_1, \ldots, s_n = t_n\} \vdash_V u = v$

11

Algebraizability から得られるもの

論理の問題を代数の問題に完全に帰着できる。universal algebra の方法や結果の利用が可能。

- 論理全体のなす束構造
- 論理的諸性質の代数的特徴づけ

すべての部分構造論理は algebraizable (Galatos - O)

12

Algebraic cut elimination

- cut elimination の持つ代数的な意味は何か？
- 決定可能性を示すために有効な cut elimination theorem の証明を algebraists に理解し易い形であたえる

シーケント $\alpha_1, \ldots, \alpha_m \Rightarrow \beta$ の provability はつぎのような代数的解釈があたえられていた。

- The inequation $\forall \bar{x}(s_1 \wedge \ldots \wedge s_m \leq t)$ follows from the axioms for HA in FOL

COE, March 2006 – p.13/1

13

Gentzen structures

では、シーケント $\alpha_1, \ldots, \alpha_m \Rightarrow \beta$ の cut-free な provability は？

- $\forall \bar{x}(s_1 \wedge \ldots \wedge s_m \preceq t)$ follows from the axioms for HA??

cut がないと $\preceq$ は transitivity を持たない

Gentzen structures の導入と、その Heyting algebras への埋め込み (quasi-embeddings)

Belardinelli-Jipsen-HO　前原、岡田等の方法の代数化

COE, March 2006 – p.14/1

14

その可能性

- cut elimination による方法の限界　— Ciabattoni-Terui, MacNeille completion と cut elimination (HO)
- proof-search が有限ステップで fail $\longmapsto$ 有限な counter-model の生成 — 岡田、BJO
- 証明法としての algebraic proof — e.g. action logic, non-associative logics

COE, March 2006 – p.15/1

15

2005 年における研究成果

- The 9th Asian Logic Conference, August 2005, Novosibirsk.
- Trends in Logic III Conference in memoriam A. Mostowski, H. Rasiowa, C. Rauszer, September 2005, Warszawa & Ruciane-Nida.
- 第２回システム検証の科学技術シンポジウム, October, 2005, 産総研　システム検証研究センター.

国際会議 Algebraic and Topological Methods in Non-Classical Logics II (June, 2005, Barcelona) の chair

COE, March 2006 – p.16/1

16

2006 年における研究活動

- N. Galatos, P. Jipsen, T. Kowalski, HO, Residuated Lattices: an algebraic glimpse at substructural logics ("Studies in Logic and the Foundations of Mathematics", Elsevier) の出版
- The 3rd Workshop of Algebra & Substructural Logics (November 2006, Krakow, Poland) の開催 (cochair)

COE, March 2006 – p.17/1

17

法律知識の矛盾の発見・解消を行う論理システム

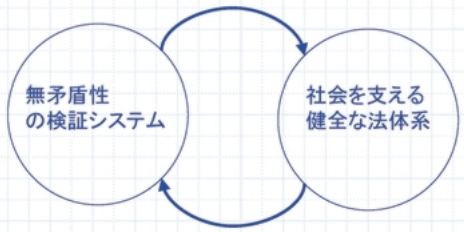
東条　敏
北陸先端科学技術大学院大学 情報科学研究科

法律知識の矛盾の発見・解消を行う論理システム

北陸先端科学技術大学院大学
情報科学研究科
東条 敏

1

安心電子社会のための法体系



2

contents

1. 法律推論とはどんなものか.
2. 無矛盾性とは何か
   i. 否定辞(¬)の問題
   ii. 含意(→)の問題
3. 非単調推論(信念修正と囲い込み)
4. 新しい論理による推論
   テーマ1 相対的否定
   テーマ2 関連性の論理
5. まとめ

3

これまでの法律推論システム

◆述語論理に基づくエキスパートシステム
◆ルール・ベースの推論システム
◆事例ベースの推論システム
◆マルチエージェントによる論争システム
◆類似性検証
◆関連性の論理・時間の論理

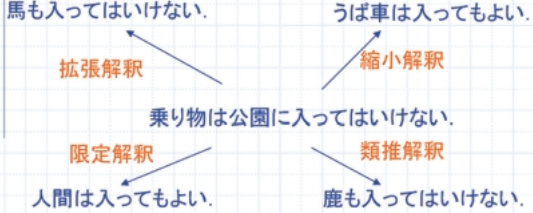
4

例えば法律の文を見てみると

◆「乗り物は公園内立ち入り禁止」
∀x[乗り物(x)→¬入園可(x)]
◆「うば車なら公園に入ってよい」
∀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)]

5

解釈の幅



6

無矛盾性の検証システム

◆既存の法律知識データベース（法律の規則群，判例集）の無矛盾性検証
◆ 更新，改正，修正にともなう無矛盾性検証

7

(i) 否定辞(¬)の問題

◆防衛行為は正当である．
∀x[行為(x)∧防衛(x)→正当(x)]

◆防衛行為は罪にはあたらない．
∀x[行為(x)∧防衛(x)→¬罪(x)]

8

(ii) 含意(→)の問題

◆{A→B, A→¬B}は矛盾ではない！
{A}を追加して初めて矛盾{B∧¬B}
が検出される．⇒ 最小の起爆剤と最小の矛盾領域の決定．
◆'→'の意味を洗い直す．
・直観主義論理 ¬¬AであってもAとは限らない．
・関連性の論理 →の両辺では因果関係がなければならない．

9

二重否定と含意の関係

◆「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)]
◆「うば車は乗り物でないとは言えない」
∀x[うば車(x)→¬¬乗り物(x)]
しかし ¬¬乗り物→乗り物 ではない

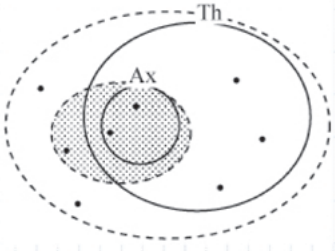
10

非単調論理

◆信念(不確かな知識)の修正 (belief revision)
- 知識の拡大(expansion)
- 知識の修正(revision)
- 知識の縮小(contraction)

◆知識の囲い込み(Circumscription)

11



12

信念の修正

α ヨーロッパの白鳥はみな白い
β 罠に捕らえられた鳥は白鳥である
γ 罠の鳥はスウェーデンから飛来した
δ スウェーデンはヨーロッパの一部である
＋
「罠の中の鳥は黒である」？？

$\alpha \sim \delta$ のどれかを棄却しなければならない．
どれを棄却すればよいか．

13

知識の囲い込み

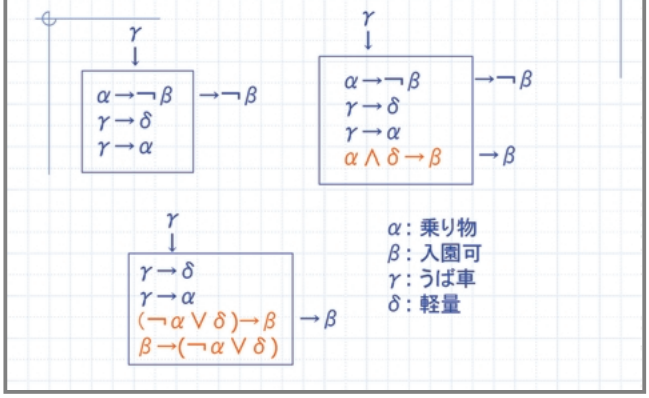
車馬の入園を禁止する．しかし軽量なるものは
この限りではない

乗り物(x)→¬入園可(x)
乗り物(x)∧軽量(x)→入園可(x)

↓「通行可」なるものの囲い込み

入園可(x)→¬乗り物(x)∨(乗り物(x)∧軽量(x))

14



15

テーマ1. 相対的否定

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

ϕに関してΔはψを否定する
⇒ 従来の否定より弱い否定

16

If $\Psi = \{\neg\beta, \gamma\}$, then $\Psi \nvdash \neg_{\alpha}\beta$.

"自分はβを偽であると知っているが，検察側がαであるという事実を知らない限りその情報は隠すことができる．"

17

$$\Delta = \{\neg\alpha, \neg\beta, \neg\gamma\}$$
$$\Gamma = \{\neg\alpha, \beta, \gamma\}$$
$$\Phi = \{\alpha, \beta, \gamma\}$$

$\Delta \vdash \neg\beta$
$\Delta \nvdash \neg_{\alpha}\beta$, because $\Delta \nvdash \alpha$

18

α minimally negates β, $\Delta \vdash \ominus_\alpha \beta$, iff:

$$\begin{cases} \Delta \vdash \neg_\alpha \beta, \ and \\ For \ any \ \varphi \ s.t. \ \Delta \vdash \neg_\varphi \beta, \\ \vdash \varphi \to \alpha \ implies \ \vdash \alpha \equiv \varphi. \end{cases}$$

ex. α does not minimally negates β, but γ does. when:

$$\Delta = \{\alpha, \ \alpha \to \gamma, \ \gamma \to \neg\beta\}.$$

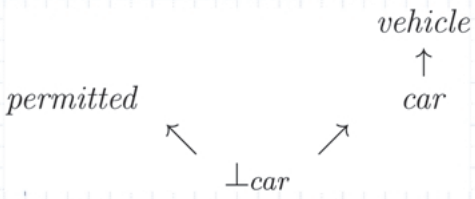
19

$\ominus^*_\alpha \beta$: The maximal x such that

$$(\alpha \to x) \wedge \neg(x \to \neg\beta).$$

$$\ominus^*_\alpha \beta = \gamma \ iff \ \alpha \to \gamma \ \wedge \ \ominus_\gamma \beta.$$

20



$$\ominus^*_{car} permitted \equiv vehicle.$$

21

テーマ2. 関連性の論理

古典論理

A→B ⇔ ¬A∨B

・前提が偽なら帰結は何であっても真？
「太陽が西から昇るなら地球は平らだ」
・帰結が真なら前提は何であっても真？
「太陽が西なら昇るなら地球は丸い」
という推論は論理的に正しくても現実的ではない.

22

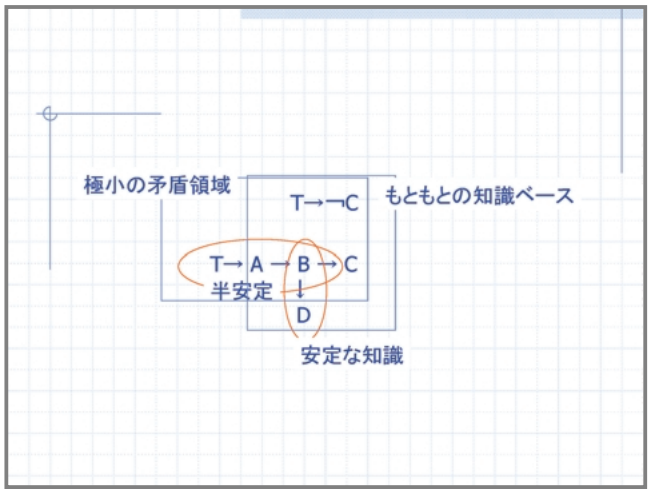
◆前提と帰結の間に命題変数の共有
Δ→「 のとき Δ∩「≠φ.
◆前提はすべて帰結に寄与する
Δ→α だからと言って Δ, β→α としない.

23

否定辞を排除した関連性推論

◆ guilty∧innocent→矛盾
◆しかし, ¬guilty→innocent ではない.
◆否定辞(¬)を除去し, 代わりに「対立」の概念を導入. 否定と矛盾を切り分ける.

24



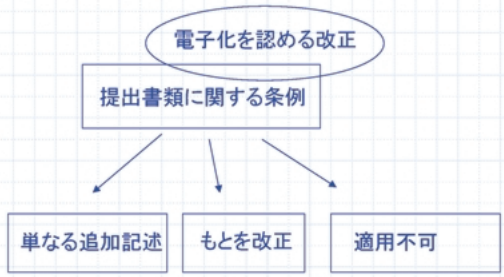
25

知識と信念の違い

◆K α → α
◆B α → α であるとは限らない
◆K ならば Cn(K) … ただし Cn(K) は K から導かれるすべての帰結

26

例 富山県の条例改正



27

まとめ

◆新しい論理を導入した法律推論システム
・否定辞の相対化
・前提･帰結関係(含意)の関連性
◆電子社会に寄与する法律の一貫性検証システム
・無矛盾性の検証システム
・矛盾を最小に修正するシステム

28

法律条文の言語処理

島津　明
北陸先端科学技術大学院大学 情報科学研究科

法律条文の言語処理

COEシンポジウム/2006. 3. 9
島津　明

1

研究内容 (2004.7 ～ 2006.2)

- 法令文の論理式への変換
  - 法令文の分析と論理式の記述
  - 変換方法の研究
    - 方式1
    - 方式2
- 法令文の見やすい表示

2

研究の位置付け

- 法令を情報処理システムの仕様とみる.
- そのため, 法令文を形式的な表現で表す.
  法令文の理解を助ける.
- それらのための言語処理をする.

3

法令文の言語処理に関する従来の研究

- 法律条文の構造のモデル化
  - 要件効果構造（田中他1993）
- 法律条文の論理表現
  - 条文を考慮した表現（吉野2000, 岡田2000）
- 法律条文の構文意味構造の解析
  - 格構造や様相表現を解析（野村他1990）

4

自然言語文の論理式への変換の従来の研究

- 日本語については本格的なシステムはない
  - 文の解釈を論理表現で記述（水谷）
- 英語では例えばDIALOGIC(SRI1982)
  1. 構文解析により構文木 . . . 拡張句構造文法
  2. 意味関数により注釈木 . . . 拡張部の関数
  3. 局所論理変換 . . . 注釈木により計算
  4. スコープの計算 . . . ヒューリスティックス
  5. プラグマティックな処理 . . . 領域依存の解釈

5

自然言語文の論理式への変換

- カテゴリをどう表現するか
  - 述語
    - *Basketball*(*b*), *Member*(*b*, *Basketball*)
  - オブジェクト
    - *Basketball*, $b \in Basketball$

6

法令文の論理表現への変換の研究

- 表現
  - 形式
  - 内容
- 変換方法
  - 返還前の文修正あるいは変換後の修正を仮定
    cf. 機械翻訳

7

法令文の論理表現の形式

- 述語論理　＋　様相記号
  - Davidosonian style
  - イベント変数
  - 格を別述語で表現（arityの問題を避ける）
- 証明器など適用する際には形式の変換も
- 様相の意味を考慮した変換も

8

法令文の論理表現の内容

- 要件効果構造
  - 要件：．．．に当たっては，．．．においては，．．．
  - 効果：．．．は　．．．しなければならない，．．．
- 要件効果構造にそって表現
  - 将来，証明器を考慮し書き換えも

9

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．（千代田区生活環境条例第2条）
  - $\forall x\, \exists e, l$ 事業者$(x) \equiv$
    （法人$(x) \vee$（団体$(x) \wedge \neg$法人$(x)) \vee$個人$(x)) \wedge$
    区内$(l) \wedge$事業活動$(e) \wedge$が$(e, x) \wedge$で(e, l)

10

表現の例

- 区は，関係行政機関と協力して，違法広告物，放置自転車等の路上障害物の除去に務めなければならない．（千代田区生活環境条例第8条）
  - O（協力$(e1) \wedge$が$(e1, b) \wedge$と$(e1, a) \wedge$
    努める$(e2) \wedge$が$(e2, b) \wedge$を$(e2, e3) \wedge$
    除去$(e3) \wedge$が$(e3, b) \wedge$
    を$(e3, x) \wedge$（違法広告物$(x) \vee$路上障害物(x)））
  - 放置自転車$(x) \supset$路上障害物(x)

（限量子は省略）

11

表現の例

- 第一項の規定を適用する場合において，前年において特別農業所得者でなかったかどうかの判定は，その年五月一日において確定しているところによるものとする．（所得税法第百十条4）
- 前年において特別農業所得者でなかった居住者は，その年五月一日の現況において，その年において特別農業所得者であると見込まれる場合には，その見込みについて，納税地の所轄税務署長の承認を求めることができる．（所得税法第百十条1）

12

表現の例

- 前年において特別農業所得者でない居住者
  - 特別農業所得者(x), . . .
  - ¬特別農業所得者(e), が(e, x), 居住者(x), time(e, 2005)
  - T(特別農業所得者(x), 2005)
    (AIMA, Russell and Norvig, reify)

13

条文の論理式への変換(手続き的)

1. 形態素解析・構文解析
2. 要件効果構造の解析
3. 関係表現の解析
4. 格構造, 名詞句意味構造
5. 部分構造の論理式への変換
6. 全体の論理式の組立て
7. 調整 (江尻, 北田)

14

条文の論理式への変換(手続き的)

- 形態素解析・構文解析
  - JUMANとKNPを使用
- 要件効果構造の解析
  - 主題部, 条件部, 対象部, 規定部を特定
  - 特徴的表現により分割

15

要件効果構造の解析

主題部・対象部

～は、	77例		
～が、	5例		
～も、	4例		

千代田区条例53号 (28条81項)
富山県条例54号 (10条21項)

条件部

～ときは、	15例	～する時に、	1例
～については、	14例	～にある時(は)、	1例
～に当たっては、	5例	～(場合)においては、	1例

文末表現(規定部)

～ことができる。	19例	～してはならない	4例	定める	4例
～する。	13例	～ものとみなす。	2例	～ない。	2例
～なければならない。	25例	～ものとする。	24例		

16

要件効果構造の解析

- 金沢市条例4号(全28項)

	主題/対象	条件	規定	述語動詞
正解	32	6	28	122
見落し	16	0	0	0
誤り	0	0	0	0

17

関係表現の解析

表現	関係	頻度
Aにより, B	原因(B, A)	1
Aため, B	目的(B, A)	7
A関し, B	関する(B, A)	3
A基づき, B	基づく(B, A)	1
AにおいてB	状況(B, A)	3
等,	(例として別式に記述)	2

18

格解析

- 動詞と名詞等の関係を解析し原始文を生成
  - 格要素が節の場合も対象
    - 「改善するよう努める」
- 法令文の分析による格フレーム辞書
  - 深層格，表層格，名詞，頻度
- 法令文の特徴を考慮した解析

19

格フレーム辞書

動詞	格	名詞	頻度
努める	が	区	3
		区長	1
		者	2
	に	活動	5
		啓発	1
		回収	1
		資源化	1
占有する	が	人	2
	を	土地	2
		建物	1
		工作物	1

20

格解析

- 構文木にそって，動詞が支配する名詞を照合
- 名詞がどの程度深層格となるかスコア付け
  - 格助詞の一致
  - 副助詞で一致
  - 文頭の「は」での一致
  - 文頭の「何人も」での一致
  - 名詞と動詞の間の読点の数
  - 名詞と事例の名詞の類似度

21

格解析

- 「広島市ぽい捨て防止条例」の格解析

品詞	正解	正解率	誤り		
			誤構文解析	辞書なし	その他
動詞(94)	52	55%	4	30	8
サ変名詞(20)	7	35%	0	7	6

22

条文の論理式への変換(機械学習)

A) 条文から注釈木(ノードに意味情報)を求める構文解析の操作を学習する方式

B) 条文と注釈木の対応を学習する方式

(Nguyen Le Minh)

23

言語処理研究開発の一般的見方

- 知識ベース/手続き的(人手による規則記述)
  - 開発時間や頑健性の問題
  - 対象領域を限定しても不完全
- 分類ベース
  - コーパス
  - 機械学習の利用
    - カーネル法，ME法等
    - 多数の素性

24

意味解析のアプローチの我々の見方

- 知識ベース/手続き的
  - 問題の分析
  - 基本的処理の考え方を与える
  - どの機械学習が適切かの指針となる
- 分類ベース
  - 頑健性
  - 多数の素性の利用による精緻化
  - コーパス/教師なし学習

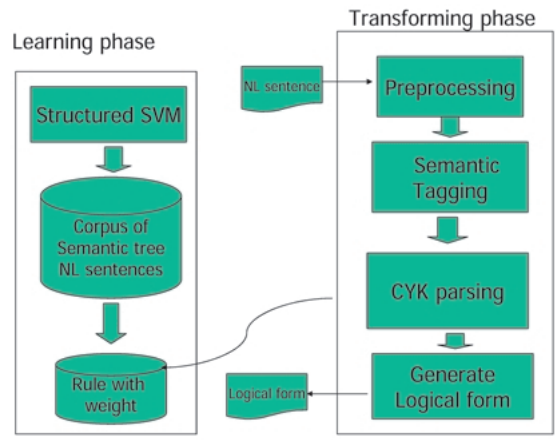
25

条文の論理式への変換(機械学習)

A) 注釈木を求める解析操作を学習
1. 注釈木を求める操作を学習し分類器を得る.
2. 分類器により入力の解析操作を求め木を得る.
3. 注釈木から論理式を組立てる.

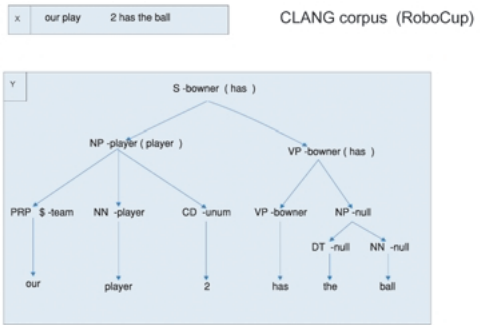
B) 文と注釈木の対応を学習
1. 文と注釈木との対応を学習し分類器を得る.
2. 分類器により入力に対する注釈木を求める.
3. 注釈木から論理式を組立てる.

26



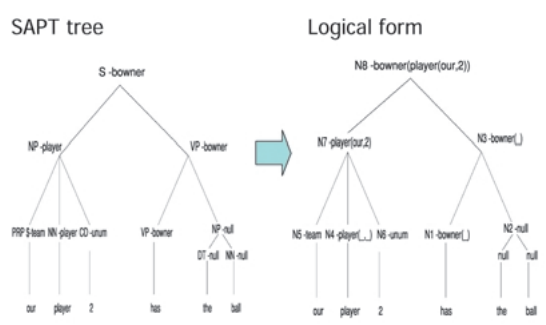
27

学習データ



28

論理表現の生成



29

実験結果

CLANG Corpus: 300文, Cross-validation test

Methods	Precision	Recall
Structure SVM	84.9	74.3
SILT (Kate, AAAI 05)	84.3	51.9
SCSISOR (Ge and Mooney CoNLL 05)	89.1	72.3

30

法令文の見やすい表示

- 法令文の特徴
- 表示システム

（山田）

31

法令文の読み方

- 条件を示す従文を読み飛ばし，主要部分をまず捉え，条件を一つづつ付加して読み直す
（田島信威「最新法令の読解法」ぎょうせい，2002）

32

法令文の読み方

実施機関は、開示請求に係る公文書の一部に非開示情報が記録されている場合において、非開示情報が記録されている部分を容易に区分して除くことができるときは、開示請求者に対し、当該部分を除いた部分につき開示しなければならない。
（富山県情報公開条例第8条第1項）

↓

実施機関は、・・・場合において、・・・ときは、・・・に対し、当該部分を除いた部分につき開示しなければならない。

33

法律条文における読点の打ち方

- 「・・・の場合において、」や「・・・ときは、」などの条件文の後には読点を打つ.
- 主文の主語の後には読点を打つが、条件文や条件句の内部の主語の後には打たない.
- 複数の名詞又は用言を並列する場合には、読点を打つ。ただし、「及び」「並びに」「又は」「若しくは」の直前の名詞の下には、読点を打たない.
- 「ただし」や「この場合において」の下には、読点を打つ.
- 「・・・であって、・・・もの、」、「・・・で、・・・もの」のように名詞を説明する場合には、説明部分が長いときや、誤読のおそれがあるときには読点を打つ.
- 対句表現の中では、対句の接続部分に読点を打ち、それぞれの対句の内部には読点を打たない.

（上田，笠井「条例規則の読み方・つくり方」学陽書房）

34

特徴的表現

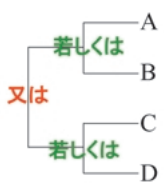
主題	～は、(50)，～も、(2)，～が、(1)
条件	～ときは、(21)，～もののほか、～て、(動詞の連用形)(3)，～を図り、～場合を除き、～場合においては、(2)，～場合であっても、～場合において、～場合にあっては、～場合は、～をし、～であって、～できるよう、～に限り、～ときを除き、～においては、～にあっては、～にかかわらず、～において、～ところにより、～に当たって、～直ちに、～にしないで、～だけで、～なく、～のほか、～の上、(1)
対象	～に対し、(17)，～について、～については、(2)，～として、～に関し、～にあっては (1)
接続	この場合において、(6)，ただし、(5)
並列	＜名詞＞、(7)，～とともに、(3)，～し、(2)，～し、及び(1)

（富山県情報公開条例54条文）

35

並列構造

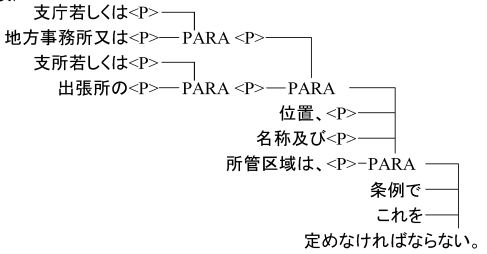
- 又は > 若しくは
  - A若しくはB又はC若しくはD
- 及び > 並びに　も同様



36

KNP式表示

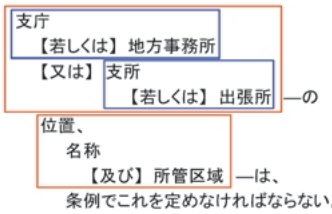
- 支庁若しくは地方事務所又は支所若しくは出張所の位置、名称及び所管区域は、条例でこれを定めなければならない。(地方自治法第155条2項)



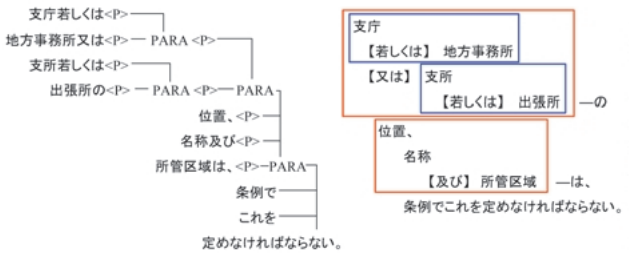
37

新表示方式

- 支庁若しくは地方事務所又は支所若しくは出張所の位置、名称及び所管区域は、条例でこれを定めなければならない。(地方自治法第155条2項)



38



39

法令文の言語処理

- 法令文の論理式への変換
  - 法令文の分析と論理式の記述
  - 変換方法の研究
- 法令文の見やすい表示

40

これから

- 別法令も加えた分析
  - 表現の正規化，限量子の扱い，
  - 条文特有の言語表現の論理表現の検討
- コーパスを増やす
- システムの改良
  - 辞書項目を増やす
- 機械学習
  - 上記研究の反映

41

CafeOBJを用いた形式手法—実行可能形式仕様言語によるシステム検証—

二木　厚吉
北陸先端科学技術大学院大学 情報科学研究科

CafeOBJを用いた形式手法
-- 実行可能形式仕様言語によるシステム検証 --

北陸先端科学技術大学院大学
情報科学研究科
言語設計学講座
JAIST-IS LDL

二木 厚吉
FUTATSUGI, Kokichi

1

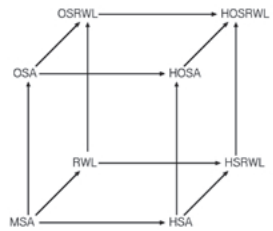
お話すること

- 形式手法とは何か？
- CafeOBJとは何か？
- CafeOBJの適用事例：電子商取引プロトコルの解析
- 今後の展望

JAIST 21COE Sympo 060310 2

2

形式手法(Formal Methods)とCafeOBJ



H : hidden
M : many
O : order
S : sorted
A : algebra
RWL : rewriting logic

3

ソフトウェア工学・システム工学における重要課題
socio-technical systems

- 要求・仕様・設計レベルでできるだけ多くの誤りを取り除く技術
  - プログラムを作ってしまってからでは修正に莫大な費用が必要になる.
- 要求・仕様・設計レベルでシステムの信頼性・安全性を確保する技術
  - システムの種類によってはテストが完全に出来ない
    - 大規模マイクロプロセッサ，航空宇宙システム
  - 実システムで事故が起こることが許されない
    - 交通システム，病院システム，金融システム…

JAIST 21COE Sympo 060310 4

4

形式手法(formal methods フォーマルメソッド)

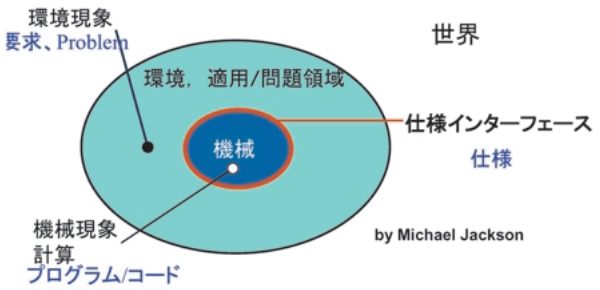
- 論理学や離散数学などに基礎をおくシステム開発法
  - 要求,仕様,プログラムを集合、関数、代数といった数学モデルに基づいて作成し解析・検証する
- 形式仕様(formal specification)に基づくシステム開発手法
  - 半自動的なシステムの検証(verification, validation)が可能になる

高信頼システム開発のための最上位の技術と位置づけられる (e.g. ITSEC)

JAIST 21COE Sympo 060310 5

5

仕様とは？ Problemとは？ Machineとは？



JAIST 21COE Sympo 060310 6

6

仕様は反駁可能であり，無矛盾性、完全性、非曖昧性、明晰性といった性質を持つことが望ましい

- 反駁可能(refutable)：真偽が客観的に決定できる記述
- 無矛盾性(consistent)： 規定されている内容に自己矛盾がない．
- 完全性(complete)： 必要な内容がすべて規定されている．
- 非曖昧性(unambiguous)： 規定されている内容が一意に特定できる．
- 明晰性(transparent)： 規定されるべき内容が理解し易く記述されている．

7

非形式仕様(Informal Specification)

- 自然語、図、ダイアグラムなどを用いて書かれた仕様のように，意味を定めるモデルや規則が与えられていない仕様
- 無矛盾性等の性質を判定する際の基準となるべき「仕様の意味」を客観的に同定することが難しく，反駁可能ではないことがある
- 無矛盾性，完全性，非曖昧性などの性質を仕様が満たすかどうか判定することが困難である
- 非形式仕様は実用上重要であるが，その性質を見極めて使うことが大切

8

形式仕様 (Formal Specification)

- あらかじめ与えられた規則に従い意味を特定することができる仕様
- 反駁可能であり，無矛盾性や正しさなどの色々な性質を仕様のレベルで解析・検証できる可能性が高い
- 計算機で処理しやすい
  - 形式言語(formal language)で書かれる
- 学習が必要：基礎理論，言語，記述の仕方．．．ちょうどプログラム言語を学習するように

9

形式仕様言語とプログラム言語

- 形式仕様言語
  - ＝(人間の)思考の道具としての言語
- プログラミング言語
  - ＝(計算機への)命令を伝える道具としての言語
- 形式仕様言語は計算機言語の高級化の延長線上にある
  - 関数型言語
  - 論理型言語
  - 代数仕様言語
  - 知識表現言語
  - UML (Unified Modeling Language)

CafeOBJは形式仕様言語

10

CafeOBJ

(Executable Algebraic Formal Specification Language： 実行可能代数仕様言語)

- JAIST二木研究室を中心に10年以上にわたり国際的なチームで研究開発
- CafeOBJ Cube(順序ソート代数，隠蔽代数，書き換え論理…)にもとづく実行可能な形式仕様言語システム
  - ->ラッピッドプロトタイピング，対話型検証
  - VDM/Zは実行可能ではない
- 等式論理に基づく簡明な対話型の検証ができる Light weight formal method
  - PVS,Isabel/HOL,Coq などはhigher-order logicに基づいており heavy (users are supposed to be familiar with math. of proofs)
  - 「何を仮定して何が検証できるのか」に関して透明度が高い (traceability)

CafeOBJ official home page:
http://www.ldl.jaist.ac.jp/cafeobj/

11

CafeOBJ適用の3つのレベル

1. 形式仕様(formal spec)を開発する；形式モデルを作る；形式仕様言語で仕様を作成する
2. 記号実行(対話的な実行，シミレーション，ラッピドプロトタイピング)等により，仕様の性質をチェックする．
3. 証明スコア(Proof Score)の実行による対話的な検証
   - Reduction(簡約,書換え)により仕様の性質を検証する

問題と状況に応じて，適切なレベルを選択する

12

CafeOBJによる検証

検証とは、仕様 *SP* が性質 *P* を満たすことを示すこと

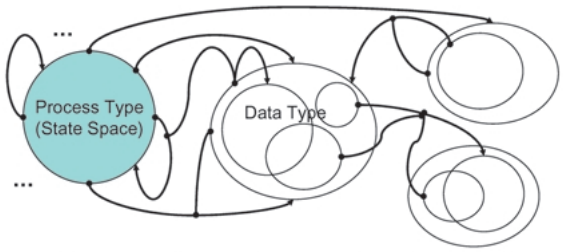
仕様 *SP* が性質 *P* を満たすとは、仕様 *SP* の任意のモデル *M* が性質 *M* を満たすこと

仕様 *SP* のモデルとは、仕様 *SP* で記述されたすべての条件(公理)を満たすモデルのこと

モデルとは、仕様に現れるものの集まり(type, sort)とその上に定義された操作・演算(operation, function)を持つ数学的なシステム(algebra)

13

Mathematical model of CafeOBJ: order-sorted algebra



All functions (operators) are postulated to be total.

14

An example of Proof Score in CafeOBJ

An Identify-Friend-or-Foe (IFF) protocol

1. check P --> Q : R
2. reply Q --> P : E_K(R,Q)

[Demonstration]

15

CafeOBJの適用事例

- 分散アルゴリズム
- コンポーネントウェア
  - Java Beans
- 鉄道信号システム
- UML(Unified Modeling language)の意味論
  - classDiagram+sOCL
- 認証プロトコル
  - NSPK,STS
- 電子商取引プロトコル
  - iKP, SET, NetBill, SSL
- セキュア・ワークフローモデル
  - Role-based workflow models
- システムバイオロジー(細胞内の化学変化・反応の記号モデルとその解析)
- Domain Engineering and Digital Rights (DEDR)

16

CafeOBJを用いた電子商取引プロトコルの解析

17

解析・検証したプロトコル(1)

- iKP (i = 1,2,3)
  - 1995年にIBMで設計;SETに影響を与えたものの1
  - 「(獲得)銀行が支払を許可するとき、必ず売り手と買い手はそれに同意している」, ということの反例を発見.
  - 修正2KPと修正3KPが上記性質を有することを検証.
- Horn-Preneel小額支払プロトコル
  - Horn(Siemens)とPreneel(Katholike Universiteit Leuven)により設計(ESORICS98で発表).
  - 売り手が過剰請求できないことを検証.

18

解析･検証したプロトコル(2)

- SET（Secure Electronic Transactions）
  - MasterCardとVISAによりプロモート.
  - 仕様書（1997年3月31日）が公開；1000ページ超.
  - 現在，支払プロトコルのモデルを作成中.
- NetBill
  - 1995年にCMUで設計.
  - 音楽，映像等のネットワークで配送可能な商品の売買の支援.
  - 商品の配送と支払いの関係を強化；SET等では，商品の配送は対象外.
  - いくつかの望ましい性質を有していることを検証済
  - 論文等で有していると主張されている性質を，厳密には有していないことを発見.

19

解析の概略

- プロトコルの数学モデルの作成
  - 何を仮定するのかを明確に定式化する
  - プロトコルの振舞のモデルを振舞遷移機械として作成.
  - CafeOBJで(等式で)モデルを記述.
- モデルが望みの性質を有すことの検証
  - 性質(この検証実験ではすべてinvariant)を式で表現.
    - 例:秘密情報は漏洩しない．メッセージの送信元の保証.
  - CafeOBJで(帰納法等の)証明譜を記述し，書き換えにより等式推論で検証

20

モデル化と検証の仮定（１）

- 支払い許可を下す機関は信頼できるものが1つだけあるとする.
- 買い手と売り手はそれぞれ複数存在しており，まじめな者とそうでない者がいるとする.
  - 参加者：買い手，売り手，支払い許可を下す機関（銀行等）.
- 個々のまじめでない者(犯罪者)をモデル化するのではなく，それらの協調した振舞をモデル化する.
  - まじめでない者たちの協調した振舞を「アタック」としてモデル化する

21

モデル化と検証の仮定（２）

「アタック」は以下のことを行う：

- ネットワーク中のあらゆるメッセージの盗聴；ただし
  - 復号用の鍵を知らない場合，暗号文は復号できない
  - ハッシュ値の原文を計算できない
  - 乱数等の値を類推できない
- 盗聴により得た情報をもしたとメッセージの偽装；ただし，
  - 暗号用の鍵を知らない場合，暗号文を生成できない.
  - 電子署名用の鍵を知らない場合，電子署名を生成できない.

つまり，ネットワークはオープンであり（インターネットのように），プロトコルで使用する暗号系はやぶられることはないことを仮定している.

22

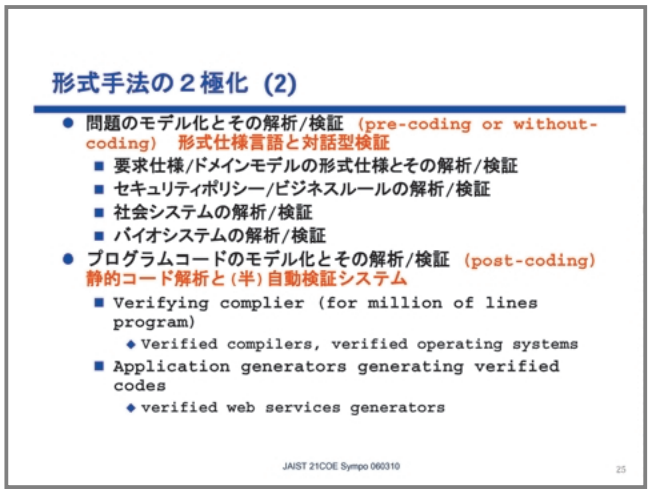
今後の展望

23

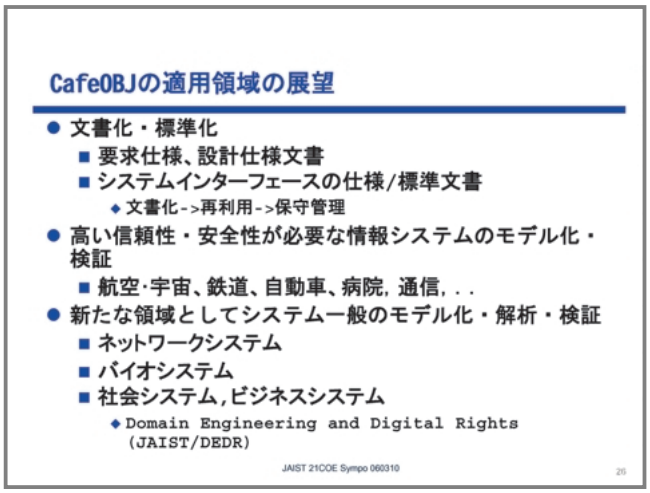
形式手法の２極化（1)

- 意思疎通と文書化の道具/技術　（形式仕様言語）
  - 要求仕様、設計仕様文書
  - システムインターフェースの標準文書
    - 文書化->再利用->保守管理
- 高い信頼性が必要なシステムの開発技術　（検証システム：モデル検査、定理証明）
  - 超高信頼性システム
    - 通信、航空･宇宙、鉄道、自動車、病院…
      - 他の技術では代替が難しい　➔　ITSECなどの標準化

24


形式手法の２極化 (2)
問題のモデル化とその解析/検証 (pre-coding or without-coding) 形式仕様言語と対話型検証
要求仕様/ドメインモデルの形式仕様とその解析/検証
セキュリティポリシー/ビジネスルールの解析/検証
社会システムの解析/検証
バイオシステムの解析/検証
プログラムコードのモデル化とその解析/検証 (post-coding) 静的コード解析と(半)自動検証システム
Verifying complier (for million of lines program)
Verified compilers, verified operating systems
Application generators generating verified codes
verified web services generators
JAIST 21COE Sympo 060310
25

25


CafeOBJの適用領域の展望
文書化・標準化
要求仕様、設計仕様文書
システムインターフェースの仕様/標準文書
文書化->再利用->保守管理
高い信頼性・安全性が必要な情報システムのモデル化・検証
航空･宇宙、鉄道、自動車、病院, 通信, . .
新たな領域としてシステム一般のモデル化・解析・検証
ネットワークシステム
バイオシステム
社会システム,ビジネスシステム
Domain Engineering and Digital Rights (JAIST/DEDR)
JAIST 21COE Sympo 060310
26

26

ビジネスプロセスの安心性検証

平石　邦彦
北陸先端科学技術大学院大学 情報科学研究科

ビジネスプロセスの安心性検証

北陸先端科学技術大学院大学・情報科学研究科
平石 邦彦

1

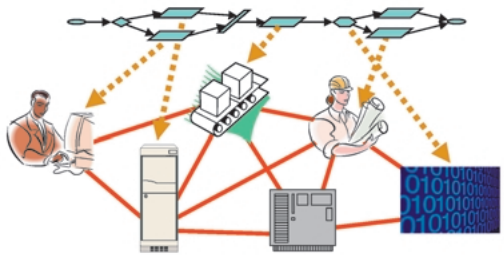
ビジネスプロセスとは

- ワークフロー
  - 業務の流れに関する順序，規則を記述したものであり，これに従って，ドキュメント・情報・タスクが，担当者から担当者へ受け渡されていくことでビジネスプロセスを自動化する．
- ビジネスプロセスモデリング
  - より進んだ形のワークフロー．あるいは，EAI(Enterprise Application Integration)の発展．
  - 異なるコンピューティング環境で稼働している複数の情報システムを統合する　→　ビジネスプロセスの追加・変更に対して情報システムも柔軟に対応できる．

2006/3/9　JAIST - COEシンポジウム2006　2

2

ビジネスプロセスとは

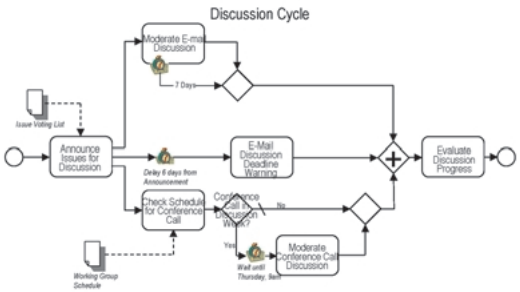


ワークフローは人，システム，情報を統合する．

2006/3/9　JAIST - COEシンポジウム2006　3

3

ビジネスプロセスのモデリング



BPMN

2006/3/9　JAIST - COEシンポジウム2006　4

4

ビジネスプロセス管理の重要性

- SOX法/サーベンス・オクスレー法
  - 企業会計や財務報告の透明性・正確性を高めることを目的に，コーポレートガバナンスの在り方と監査制度を抜本的に改革するとともに，投資家に対する企業経営者の責任と義務・罰則を定めた米国連邦法(@IT情報マネジメント用語辞典)．
  - 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．
  - 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．

2006/3/9　JAIST - COEシンポジウム2006　5

5

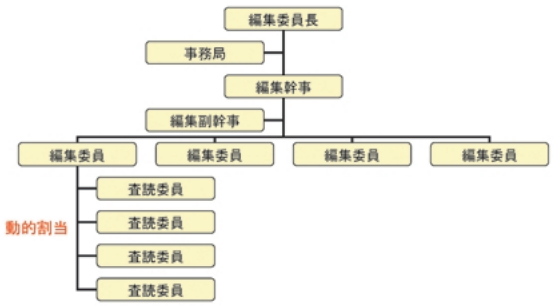
ビジネスプロセスの安心性検証

- 事前の検証，実行時の継続的なモニタリング ⇒ 安心性
- 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．

2006/3/9　JAIST - COEシンポジウム2006　6

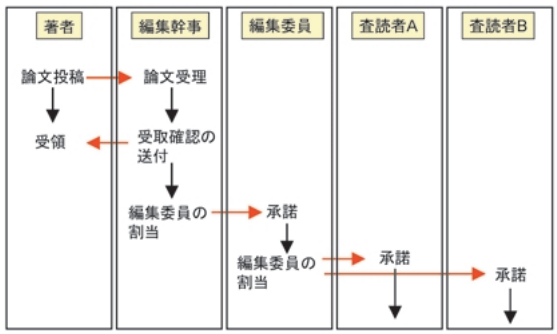
6

例題：論文査読プロセス ― 組織図



7

例題：論文査読プロセス ― ワークフロー



8

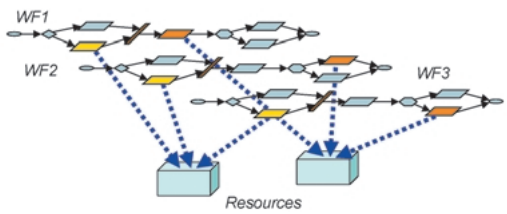
例題：論文査読プロセス ― 規則

- 編集幹事は，新規投稿論文に対して担当編集委員を選定する．
- 担当編集委員は，担当論文に対し適当な査読委員（2名）を選定する．
- 不採録論文が再投稿された場合，原則として前回と同じ編集委員及び査読委員が担当する．
- 投稿者と同一機関に所属する者を担当編集委員または担当査読委員には選定しない．
- 同一人への査読割当件数は，5件以内となるよう割当の平均化を図る．
- 同一著者から投稿された複数の関連する論文については，3編までを，同一査読委員に割当てることができる．

9

ワークフローの性能評価

- ワークフローはテンプレートであり，実際には多くのインスタンスがシステム上で動作する．
- 与えられた性能基準を満たすために，適切な資源配分を行う必要がある．



10

最適資源配分問題

査読プロセスのワークフローにおいて，論文投稿数に対して適切な編集委員の数を求めよ．

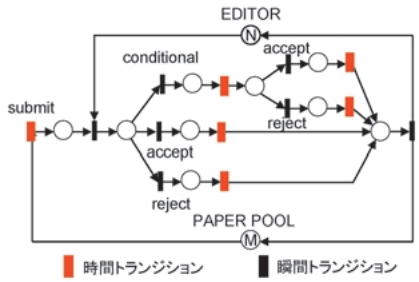
11

査読プロセスの統計データ

- 投稿から最終結果通知までの時間
  - 1回目査読後採録: 2.4月
  - 1回目査読後不採録: 3.9月
  - 2回目査読後採録: 5.9月
  - 2回目査読後不採録: 6.8月
- 採録／不採録率
  - 1回目査読後採録: 0.065
  - 1回目査読後不採録: 0.687
  - 2回目査読後採録: 0.238
  - 2回目査読後不採録: 0.010
- 投稿数: 16.9/月

12

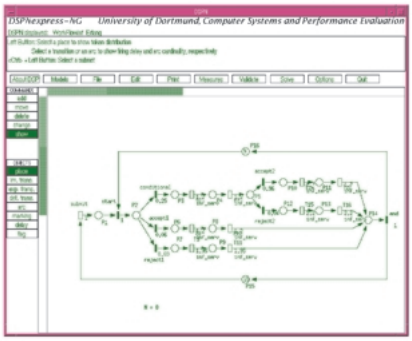
査読プロセスの性能評価モデル



一般化確率ペトリネット(GSPN)

13

確率ペトリネットのツール



14

査読プロセスの性能評価モデル ー 解析結果

N	状態数	計算時間(秒)	処理待ちトークン数の期待値
3	2926	0.083	10.18
4	8866	0.202	5.94
5	23023	0.544	1.99
6	53053	1.787	0.63
7	110968	4.803	0.21
8	213928	8.882	0.008
9	384098	19.684	0.003

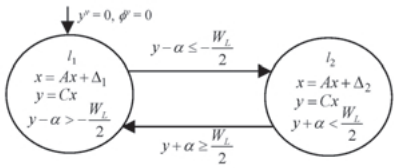
Itanium2 1.6GHz/9MBCache, 16GB Memory

1トークン＝論文16.9
N = 8 ⇒ 8×16.9 = 135.2 本の処理能力
1人あたり最大5本の処理能力とすると，編集委員数 = 135.2/5 = 27.04 人

15

ハイブリッドシステムによる近似

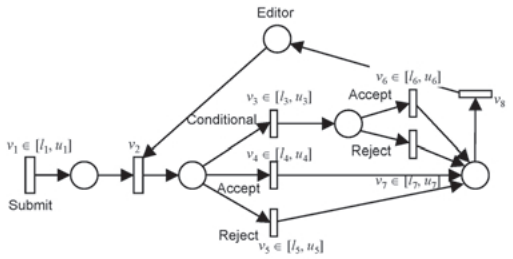
- ハイブリッドシステム
  - オートマトンにより記述されるデジタル動作(離散事象系)と微分方程式により記述されるアナログ動作(連続系)が混在するシステム.



ハイブリッドオートマトン

16

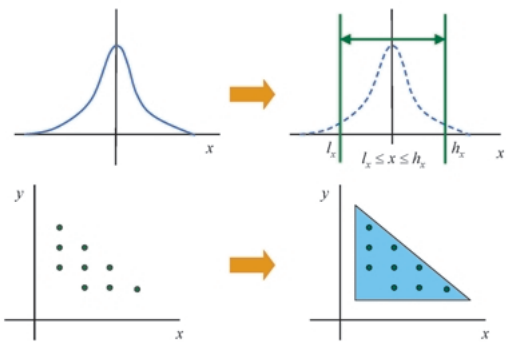
連続ペトリネットによる近似



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.

17

連続ペトリネットによる近似



18

ハイブリッドシステム表現を用いたワークフローの解析

- 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.

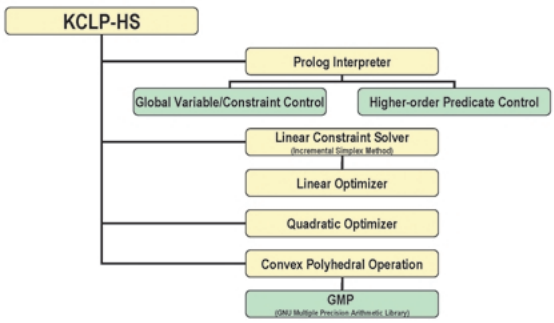
19

成果

- 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).
- 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.
- 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.

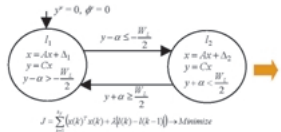
20

KCLP-HS



21

KCLP-HS



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

22

KCLP-HS

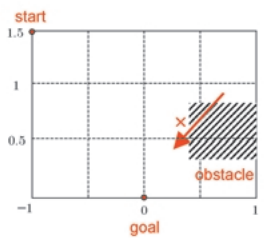
$$x(t+1) = 0.8\begin{bmatrix}\cos\alpha(t) & -\sin\alpha(t)\\ \sin\alpha(t) & \cos\alpha(t)\end{bmatrix}x(t) + \begin{bmatrix}0\\1\end{bmatrix}u(t)$$

$$y(t) = \begin{bmatrix}1 & 0\end{bmatrix}x(t)$$

$$\alpha(t) = \begin{cases}\pi/3 & \text{if } \begin{bmatrix}1 & 0\end{bmatrix}x(t) \geq 0\\ -\pi/3 & \text{if } \begin{bmatrix}1 & 0\end{bmatrix}x(t) < 0\end{cases}$$

$$x(t) \in \begin{bmatrix}-10 & 10\end{bmatrix} \times \begin{bmatrix}-10 & 10\end{bmatrix} \; u(t) \in \begin{bmatrix}-1 & 1\end{bmatrix}$$

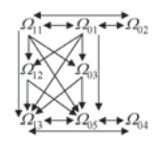
$$J_k(x_0, x_f, u) = \sum_{t=0}^{k-1} \|u(t)\|_{Q_1}^2 + \|x(t) - x_f\|_{Q_2}^2$$



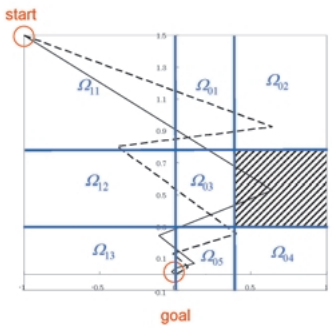
最適制御問題

23

KCLP-HS



Discrete State Transition



24

進行中

- ハイブリッドシステム表現を用いたビジネスプロセスの性能検証.
- 担当者の動的割当を許すワークフローシステムの検証問題（日立Cosminexusワークフローシステムへの実装）.

25

今後

- ドメインモデル記述とビジネスプロセスの整合性検証.
- ビジネスプロセスのモニタリング手法 ー オンライン検証.

26

モデル化と証明に基づく電子社会の安心性検証

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

モデル化と証明にもとづく
電子社会の安心性検証

Verifiable trustworthy e-society based on model construction and proofs

小川瑞史
Mizuhito Ogawa

1

Targets and methodology

- Verification targets
  - Mathematical model
    Various logic
  - High-level design
    UML, Z
  - Program code
    Java, ML
- Methodology
  - Theorem prover
    Isabelle, MONA
  - Model checker
    Weighted PDS

Manual model construction

Automatic model construction

Use existing tools / theory as much as possible

2

Recent work related verification

- Temporal authentication algorithm verification (with NTT, 2005)
- Open induction library on Isabelle/HOL (2005-)
- Java analyzer by Weighted pushdown MC (2006)
- Type guided MC of security protocol (2005-6)

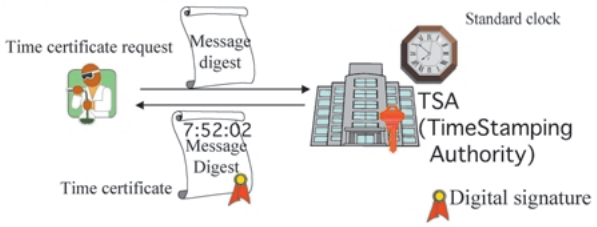
3

What is temporal authentication ?

Certificate an occurrence of an transaction at "*time*"

- Time stamp by digital signature (rfc-3161)
- Linking and publication by hash (ISO 18014-3)

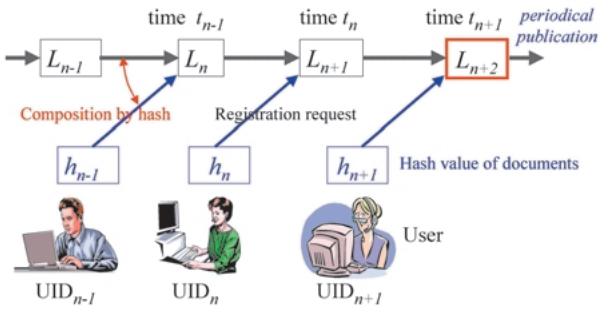
Time stamp by digital signature (rfc-3161)



4

Linking and publication by hash function (ISO18014-3)

Compose past time stamps by a hash function



We assume collision-resistance, one-way hash function.

5

Time stamp by digital signature v.s. Linking by hash

Time stamp by digital signature　　*First certificate*

Pros :
- Relatively safe for intra-dishonesty by Hardware Secure Module.
- Fine precision (< sec).

Cons:
- Contamination of crypto system invalidates *all* certificates.
- Relatively short life span : ～5years.

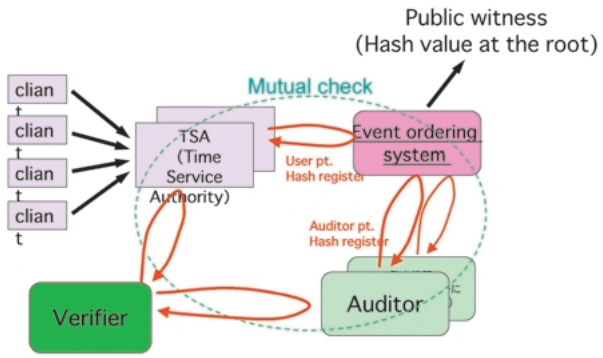
Linking and publication by hash function　　*Secondary certificate*

Pros :
- Relies only on hardness of a hash function (e.g., SHA-1).
- Relatively long life span : ～30years.

Cons:
- Hash function has no key; guarantee required for intra-dishonesty
- During publication period, no auditor can check.

6

Mutual checking mechanism



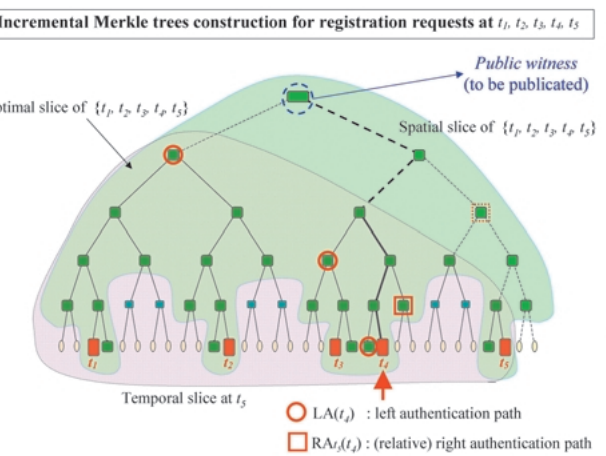
7

Merkle tree (Merkle 1979)

- *Merkle tree = Binary tree + hash function*
- Each node has its hash value, computed from a pair of hash values of its children.

We assume collision-resistance, one-way hash function.

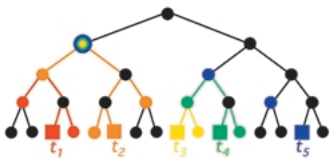
8



9

What we proved ?

- Property 1: Correctness of incremental construction
  - Manual proof known, verify with MONA
- Property 2: Correctness of Incremental sanity check
  - First manual proof, assisted by MONA



MONA: satisfiability checker for monadic second order logic

10

Recent work related verification

- Temporal authentication algorithm verification (with NTT, 2005)
- Open induction library on Isabelle/HOL (2005-)
- Java analyzer by Weighted pushdown MC (2006)
- Type guided MC of security protocol (2005-6)

11

Why open induction ?

- Understand Axiom of Choice in Isabelle/HOL.
  - Library related to Zorn's lemma
- Formal proof of Kruskal-type theorems.
  - First goal: Higman's lemma
- There may be demand for "proof".
  - 3 tries in 2005 (2 succeeded, 1 failed)

12

Higman's Lemma

- **Def.** $(A,\leqq)$ is WQO if each infinite sequence $a_1, a_2, \ldots$ has i, j such that $i < j$ and $a_i \leqq a_j$.
- ***Higman's* Lemma**. If $(A, \leqq)$ is WQO, $(A^*,\leqq)$ is WQO where $a_1\, a_2 \ldots a_m \leqq a'_1\, a'_2 \ldots a'_n$ is embedding.

e.g., $(1, 3, 2, 5) \leqq (1, 4, 0, 2, 6)$,
$\_\ (1, 2, 3, 5) \leqq (1, 4, 0, 2, 6)$,

13

History of proofs of Higman's lemma

- Higman's Lemma (1952 Higman)
- Proof by MBS (1963 Nash-Williams)
- Constructive proof in terms of ordinal (Simposon 1988)
- Variation of regular expressions (Murthy-Russel, 1990)
- A-translation (using *Nuprl*, Murthy 1990)
- Open induction (Coquand 1993, Gaser 1996)
- ....

Computational contents in classical proofs

14

Lexicographic ordering on infinite seqs

- **Def.** Assume that > is a well-founded ordering. Let $(t_1,t_2,\ldots) >_{lex} (u_1,u_2,\ldots)$ if there exists i s.t. $t_j = u_j$ for $\forall\, j < i$, and $t_i > u_i$.
- **Remark.** $>_{lex}$ *(on infinite sequences) is NOT WFO.*
- **Well founded indu** : if < is WFO, $(\forall x\, (\forall y\, (y < x \Rightarrow P\, y) \Rightarrow P\, x)) \Rightarrow (\forall x.\, P\, x)$

DOES NOT WORK !

- **Lemma.** $>_{lex}$ *is downward complete.*

15

Open induction library

- > is *downward complete*, if each nonempty descending chain has a greatest lower bound.
- *P* is *open*, if, for each descending chain $x_1 \geqq x_2 \geqq \ldots$, $P(\text{glb}\ \{x_i\})$ implies $P(x_j)$ for some j.

About 250 lines in Isabelle/HOL

- **Open Indution** If > is *downward complete* and *P* is *open*,
  $(\forall x\, (\forall y\, (y < x \Rightarrow P\, y) \Rightarrow P\, x)) \Rightarrow (\forall x.\, P\, x)$

Proper extension of well-founded induction

16

Recent work related verification

- Temporal authentication algorithm verification (with NTT, 2005)
- Open induction library on Isabelle/HOL (2005-)
- Java analyzer by Weighted pushdown MC (2006)
- Type guided MC of security protocol (2005-6)

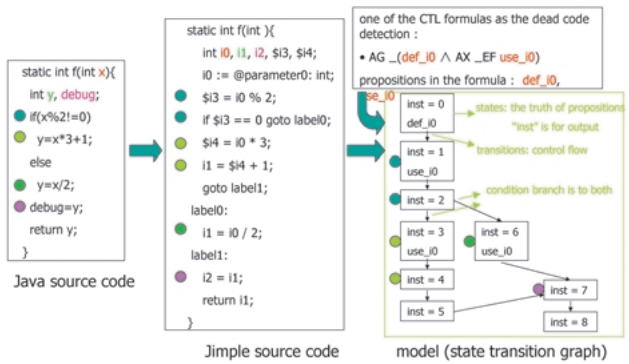
17

Analysis = Abstraction+Model checking

- Model checker as backend analysis engine.
  Example : Java dead code detection
- Old work (2003, U.Tokyo) Control flow
  Intraprocedual analysis : SOOT + SMV
  Dead code detection ($\_use_x$ **W** def_x)
  Design 2 months, Implementation 1 month (M2)
- Recent work (2006, JAIST) Dataflow
  Interprocedual analysis : SOOT + WeightedPDS
  Dead code detection (PER-based abstraction)
  Design 8 months, Implementation 2 weeks (D2)

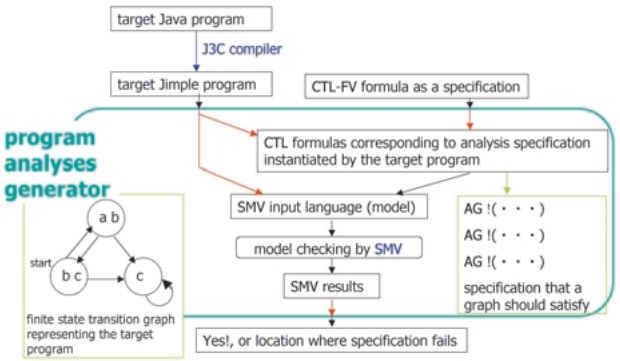
18

Example of model generation (SMV)



19

Java analyzer on SMV (Old work)



20

Java use/def dead code detection by SMV

- Abstraction (= Jimple code → SMV): 700 lines in Java
- Implement intra-procedural dead code detection (used/def method)

Java.math.* (Java 1.3.1)	bytes	Method	Time (sec)	Dead codes
SignedMutableBigIntege	1146	8	1.81	0
BitSieve	1948	10	5.77	0
BigDecimal	7217	35	26.70	0
MutableBigInteger	12966	50	167.96	11
BigInteger	28888	104	346.58	14

333MHz PenII MMX, 128MB memory, Windows98

21

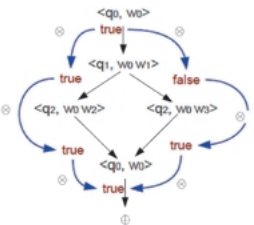
Weighted PDS (Reps, 2003)

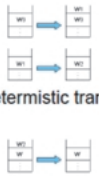
- Weighted PDS = (P, D, f) where $f: \Delta \to D$ for
  - $P = (Q, \Gamma, \Delta, p_0, \omega)$: pushdown transition system
  - D : bounded idempotent semiring (D,+,×,0,1)
- **Intuition.** Element in D is a function on properties
  - $f \times g = g \cdot f$ (on a path, f followed by g)
  - f + g (when two path meet)
- Implementations available for generalized reachability. (Weighted DPS, WPDS+)

22

Example of weighted PDS

$\langle q_0, w_0 \rangle \hookrightarrow \langle q_1, w_0 w_1 \rangle$ TRUE
$\langle q_1, w_1 \rangle \hookrightarrow \langle q_2, w_2 \rangle$ TRUE
$\langle q_1, w_1 \rangle \hookrightarrow \langle q_2, w_3 \rangle$ FALSE
$\langle q_2, w_3 \rangle \hookrightarrow \langle q_0, \epsilon \rangle$ TRUE
$\langle q_2, w_2 \rangle \hookrightarrow \langle q_0, \epsilon \rangle$ TRUE



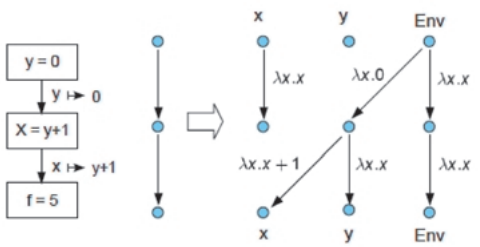


nondetermistic transition

- TRUE (=1): say, reachable
- FALSE (=0): say, unreachable
- × = ∧, + = ∨

23

Encoding dataflow by exploded supergraph

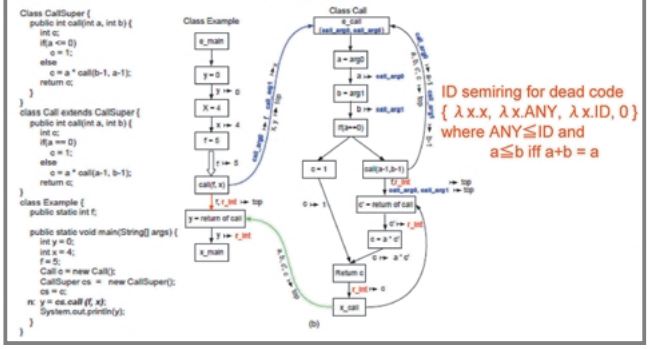


- Encoding : cl = var, stack = (pc∪return pt.)*

24

Example of model generation (WPDS)

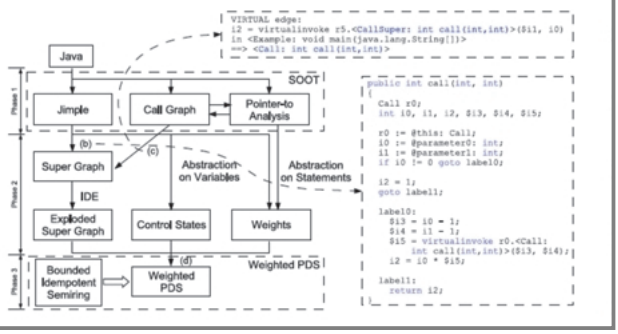
- Abstraction (= Jimple → WPDS): 1500 lines in Java
  Stack machine (pc×env, stack) ⇒ WPDS (cl, stack)



25

Java Analyzer on WPDS (recent work)

- Analysis as generalized pushdown reachability of WPDS, specified by bounded idempotent semiring



26

Publication 2005.4-2006.3

- M.Ogawa, E.Horita, S.Ono, *Proving Properties of Incremental Merkle Trees, CADE-20, 2005.*
- X.Li, M.Ogawa, *Interprocedural Program Analysis for Java based on Weighted Pushdown Model Checking, AVIS'06, 2006.*
- I.Sasano, M.Ogawa, Z.Hu, *Maximum Marking Problems with Accumulative Weight Functions, ICTAC05*, 2005.

27

Research activity 20054.-2006.3

- Organizer
  - COE workshop on Verification Technology (VERITE)
    ⇒ JAIST/AIST joint workshop (next 2006 May.19)
  - COE workshop on Theorem Proving and Provers
    ⇒ Closed workshop (next this Autumn)
  - Several COE seminars
  - 第22回日本ソフトウェア科学会大会 (PC chair)
    ⇒ 検証手法（定理証明、モデル検査）セッション

28

Future collaboration

- Proving Kruskal-type theorems on Isabelle/HOL
  - Term rewriting system theory library (Innsbruck U.)
- Analysis implementation = IML + abstraction + MC
  - SML# compiler (Ohori, Tohoku U.)
- Modeling realtime system and its verification (?)
  - Composability / Asynchronicity (Ono, Kogakuin U.)

29

ソフトウェアアカウンタビリティの定義と実現法

落水　浩一郎
北陸先端科学技術大学院大学 情報科学研究科

ソフトウェアアカウンタビリティ
の定義と実現法

（電子社会のモデル化と進化グループ）

落水　浩一郎
北陸先端科学技術大学院大学　情報科学研究科
JAIST　21世紀COEシンポジウム2006
2006年3月9日

1

研究の目指すもの

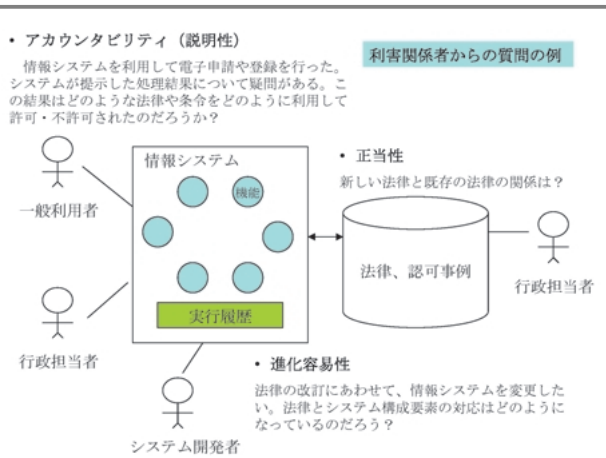
- 電子社会における安心性要件のうち、アカウンタビリティと進化容易性について、以下の機能を実現するための理論と実現法を開発する。
  - 様々な利害関係者からの質問に、彼等のセマンティクスと言語を利用して答えうる機能
  - 規則の改訂に対応して適切に進化できる情報システムの構造、および、それらの進化を支援する機能

2

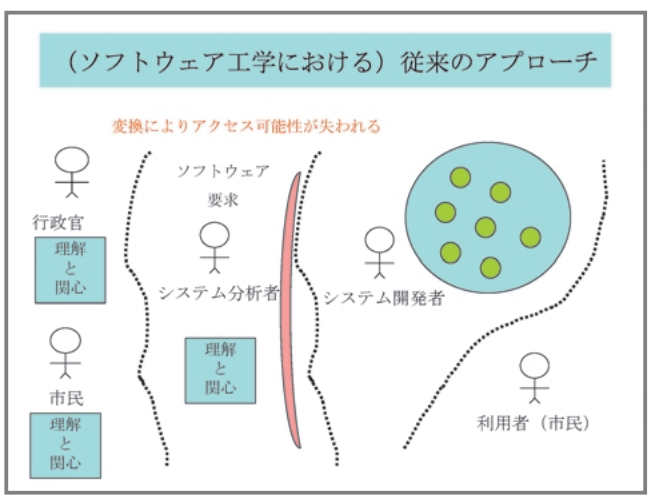
利害関係者とは

- 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存在する。例えば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場合、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。
  - 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。
  - 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。

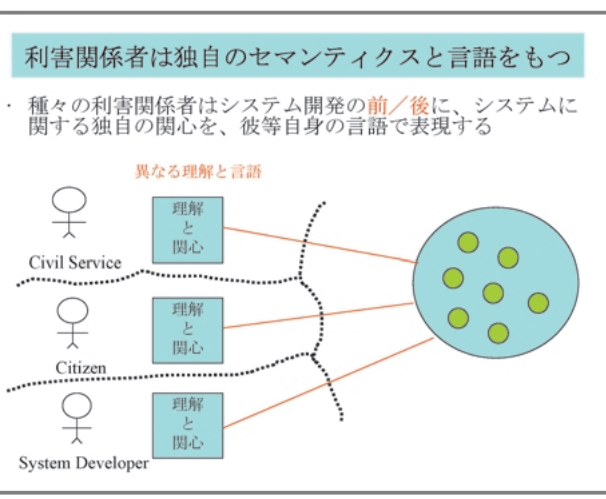
3



4

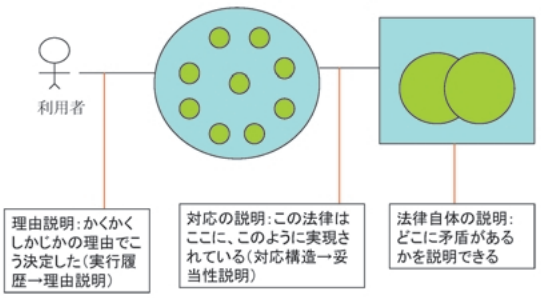


5



6

３種のアカウンタビリティ



7

我々のグループの研究範囲

- 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。以下の２点を対象とする。
  - 検証済みの法律（または規則）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を開発する（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

8

進化容易性については

- 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に関する研究成果を背景にして、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予定である。

9

現在までの成果

- 原因結果グラフを用いた自己説明モジュールの設計
- 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

10

自己説明モジュールの設計

- 本学の履修規則、および、ある会社の社内規則（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（原因と結果関係の因果関係をＡＮＤ／ＯＲ木で表現したもの）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

11

決定表の例

- 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

12

適用事例の特徴

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。

13

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

- Law-Defined Systemを対象とする
- 3層モデルと自己説明モジュールを「インターセプタ・プロキシ」により結合する。
- 自己説明モジュールは、インターセプタに保持される、既存システムの実行履歴と追加の質問をもとに答えを特定する
- 既存システムはサブシステムの呼び出しをインターセプタを介して行うので、その部分だけ再コンパイルする必要がある。

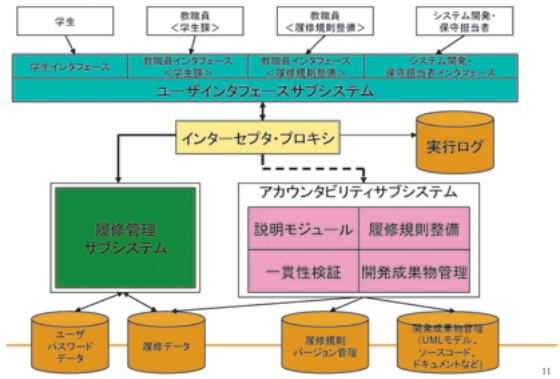
14

Law-Defined Systemとは

- 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（情報システムの要求仕様）を完全にみ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できる情報システムをLaw-Defined Systemと呼ぶ

15

履修管理システムのアーキテクチャ



16

今後の課題

- JAIST履修管理システムを実現する。社内規則および履修規則に関する自己説明モジュールを実現する
- 機能性を検証する
- 検証グループの成果と融合させ、自己説明モジュールの自動生成をはかる
- オントロジーを整備しつつ、履修規則と社内規則に共通するルールを洗い出す。
- フィールドテストののち、富山県の地方自治体システムに成果を適用する

17

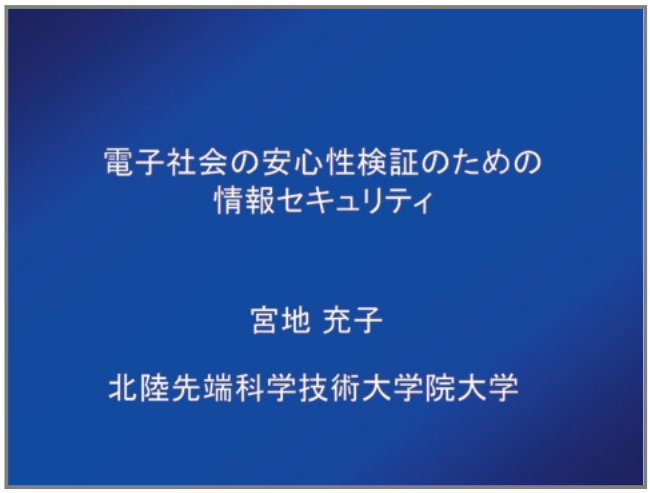
発表論文

- [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.
- [4] 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.,2006 .

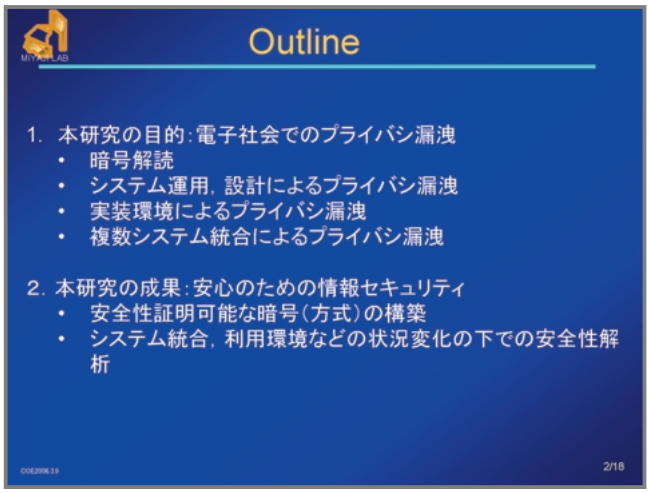
18

電子社会の安心性検証のための情報セキュリティ

宮地　充子
北陸先端科学技術大学院大学 情報科学研究科

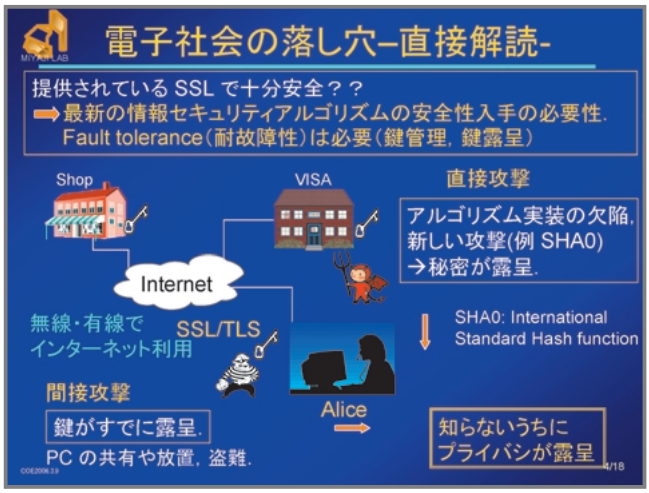


1

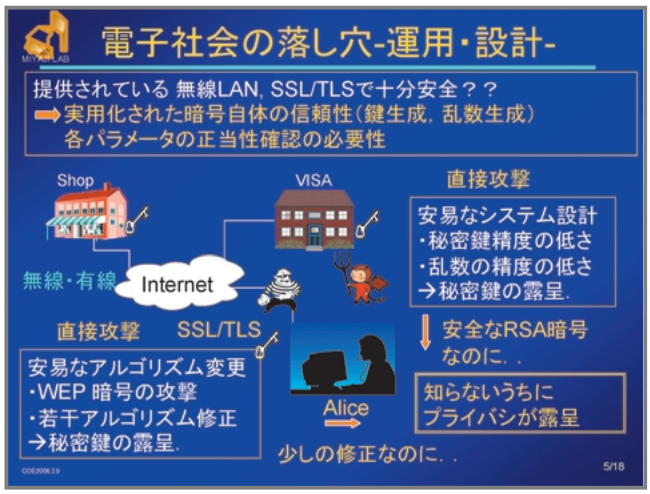


2

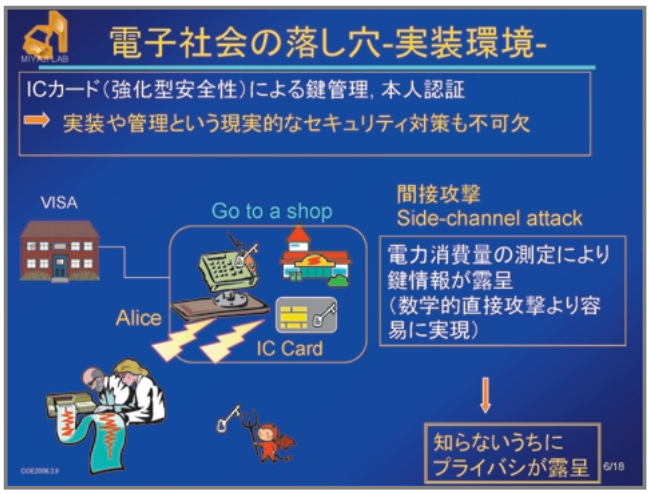
3



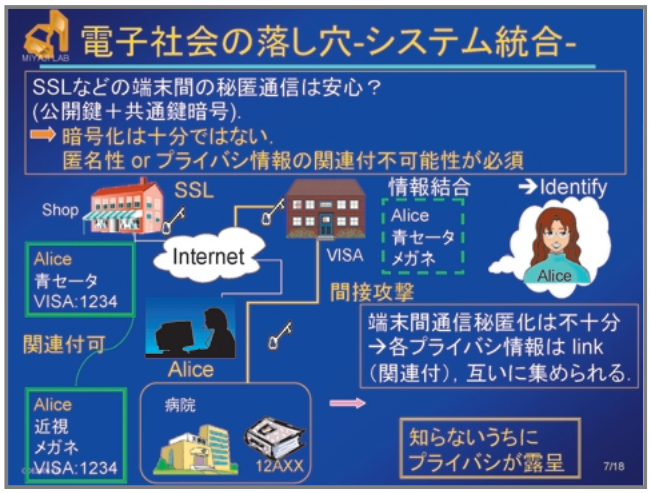
4



5



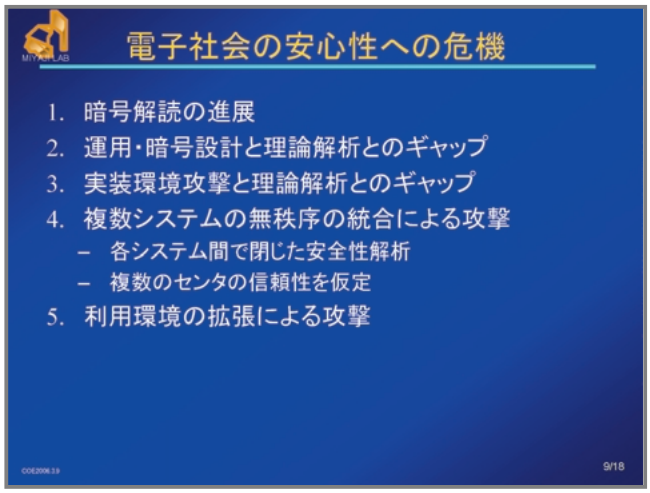
6


電子社会の落し穴-システム統合-
SSLなどの端末間の秘匿通信は安心？
(公開鍵＋共通鍵暗号).
➡ 暗号化は十分ではない.
匿名性 or プライバシ情報の関連付不可能性が必須
Shop
SSL
Internet
VISA
情報結合
Alice
青セータ
メガネ
➔Identify
Alice
Alice
青セータ
VISA:1234
関連付可
間接攻撃
端末間通信秘匿化は不十分
➔各プライバシ情報は link
(関連付), 互いに集められる.
Alice
Alice
近視
メガネ
VISA:1234
病院
12AXX
知らないうちに
プライバシが露呈
7/18

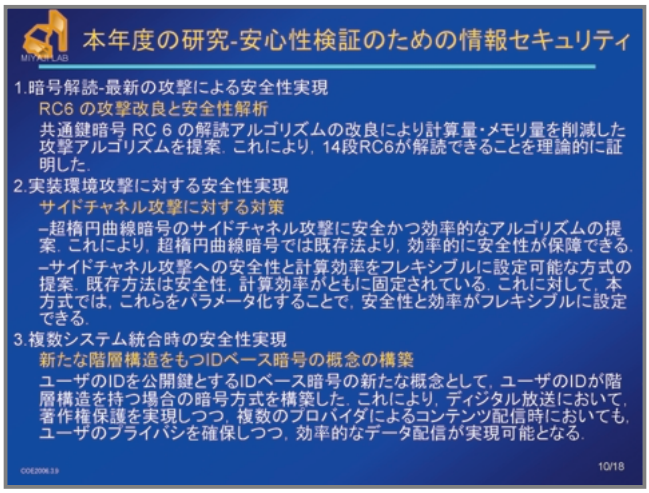
7


電子社会の落し穴 -利用前提の拡張-
プライバシ情報の電子化　位置情報, 思考・趣向情報
➡ 匿名性 と関連付不可能性が必須
home 12AXX – ホラー
Back to home
関連付可
Shop
12AXX – ホラー
Go to a shop.
Hospital
12AXX – ホラー
Go to a hospital with a book
RFID
12AXX-ホラー
図書館
RFIDによる本管理
8/18

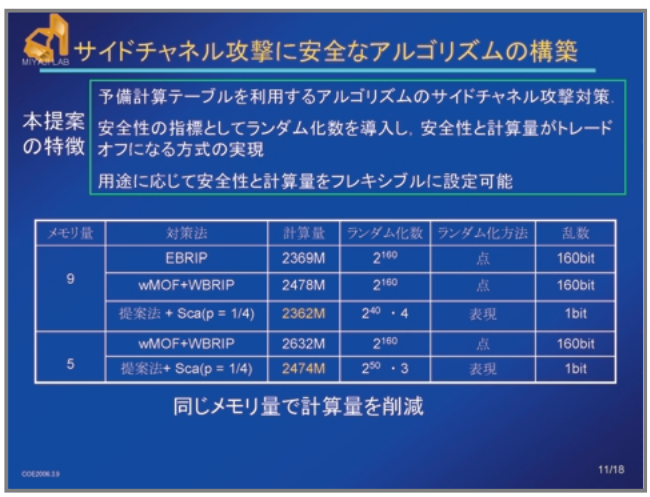
8


電子社会の安心性への危機
1. 暗号解読の進展
2. 運用・暗号設計と理論解析とのギャップ
3. 実装環境攻撃と理論解析とのギャップ
4. 複数システムの無秩序の統合による攻撃
– 各システム間で閉じた安全性解析
– 複数のセンタの信頼性を仮定
5. 利用環境の拡張による攻撃
9/18

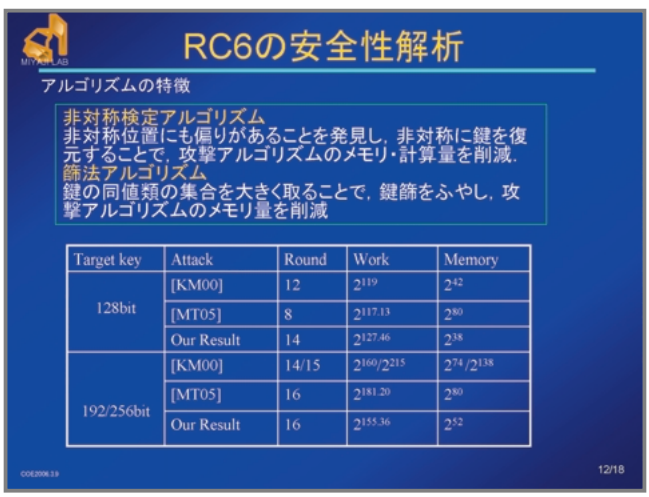
9


本年度の研究-安心性検証のための情報セキュリティ
1.暗号解読-最新の攻撃による安全性実現
RC6 の攻撃改良と安全性解析
共通鍵暗号 RC 6 の解読アルゴリズムの改良により計算量・メモリ量を削減した攻撃アルゴリズムを提案. これにより, 14段RC6が解読できることを理論的に証明した.
2.実装環境攻撃に対する安全性実現
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の提案. これにより, 超楕円曲線暗号では既存法より, 効率的に安全性が保障できる.
–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の提案. 既存方法は安全性, 計算効率がともに固定されている. これに対して, 本方式では, これらをパラメータ化することで, 安全性と効率がフレキシブルに設定できる.
3.複数システム統合時の安全性実現
新たな階層構造をもつIDベース暗号の概念の構築
ユーザのIDを公開鍵とするIDベース暗号の新たな概念として, 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となる.
10/18

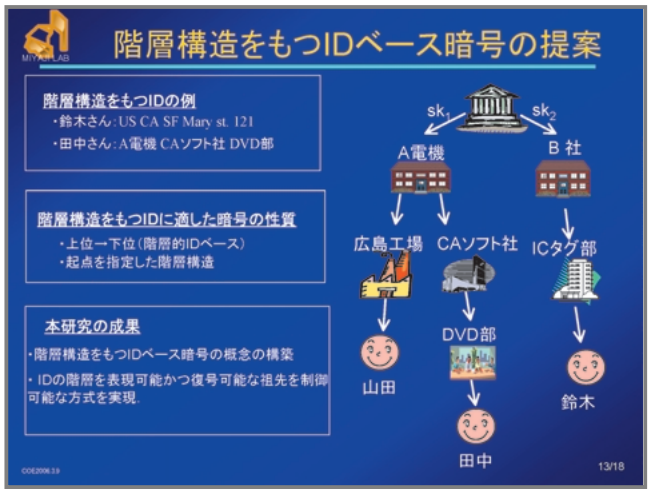
10


サイドチャネル攻撃に安全なアルゴリズムの構築
本提案の特徴
予備計算テーブルを利用するアルゴリズムのサイドチャネル攻撃対策.
安全性の指標としてランダム化数を導入し, 安全性と計算量がトレードオフになる方式の実現
用途に応じて安全性と計算量をフレキシブルに設定可能
メモリ量 | 対策法 | 計算量 | ランダム化数 | ランダム化方法 | 乱数
9 | EBRIP | 2369M | 2^{160} | 点 | 160bit
9 | wMOF+WBRIP | 2478M | 2^{160} | 点 | 160bit
9 | 提案法 + Sca(p = 1/4) | 2362M | 2^{40} ・4 | 表現 | 1bit
5 | wMOF+WBRIP | 2632M | 2^{160} | 点 | 160bit
5 | 提案法+ Sca(p = 1/4) | 2474M | 2^{50} ・3 | 表現 | 1bit
同じメモリ量で計算量を削減
11/18

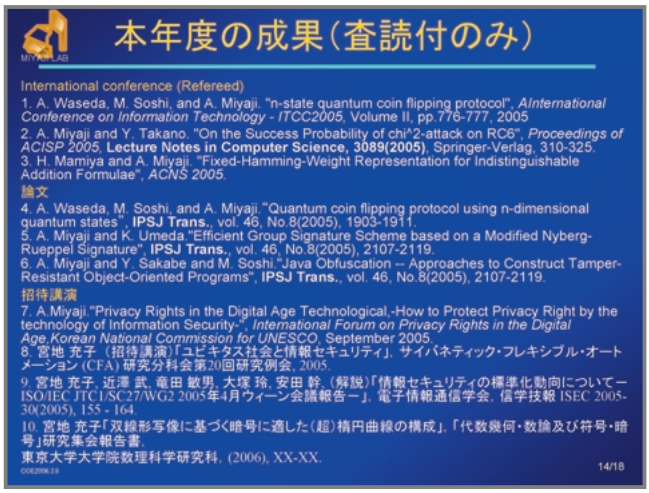
11


RC6の安全性解析
アルゴリズムの特徴
非対称検定アルゴリズム
非対称位置にも偏りがあることを発見し, 非対称に鍵を復元することで, 攻撃アルゴリズムのメモリ・計算量を削減.
篩法アルゴリズム
鍵の同値類の集合を大きく取ることで, 鍵篩をふやし, 攻撃アルゴリズムのメモリ量を削減
Target key | Attack | Round | Work | Memory
128bit | [KM00] | 12 | 2^{119} | 2^{42}
128bit | [MT05] | 8 | $2^{117.13}$ | 2^{80}
128bit | Our Result | 14 | $2^{127.46}$ | 2^{38}
192/256bit | [KM00] | 14/15 | $2^{160}/2^{215}$ | $2^{74}/2^{138}$
192/256bit | [MT05] | 16 | $2^{181.20}$ | 2^{80}
192/256bit | Our Result | 16 | $2^{155.36}$ | 2^{52}
12/18

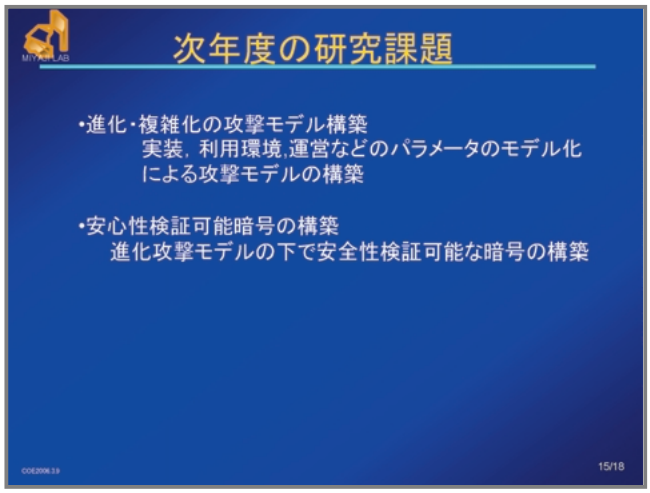
12


階層構造をもつIDベース暗号の提案
階層構造をもつIDの例
・鈴木さん：US CA SF Mary st. 121
・田中さん：A電機 CAソフト社 DVD部
階層構造をもつIDに適した暗号の性質
・上位ー下位（階層的IDベース）
・起点を指定した階層構造
本研究の成果
・階層構造をもつIDベース暗号の概念の構築
・IDの階層を表現可能かつ復号可能な祖先を制御可能な方式を実現.
sk1
sk2
A電機
B 社
広島工場
CAソフト社
ICタグ部
DVD部
山田
鈴木
田中
13/18

13


本年度の成果（査読付のみ）
International conference (Refereed)
1. A. Waseda, M. Soshi, and A. Miyaji. "n-state quantum coin flipping protocol", AInternational 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
4. 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.
5. 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.
6. 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
7. 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.
8. 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.
9. 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ーISO/IEC JTC1/SC27/WG2 2005年4月ウィーン会議報告ー」, 電子情報通信学会, 信学技報 ISEC 2005-30(2005), 155 - 164.
10. 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), XX-XX.
14/18

14


次年度の研究課題
•進化・複雑化の攻撃モデル構築
実装，利用環境,運営などのパラメータのモデル化による攻撃モデルの構築
•安心性検証可能暗号の構築
進化攻撃モデルの下で安全性検証可能な暗号の構築
15/18

15

Fault-tolerant group communication protocols and fault-detection for distributed systems and their application to autonomous mobile systems

Xavier Defago
北陸先端科学技術大学院大学 情報科学研究科

Group Communication and Fault-Detection for Distributed Systems with Application to Autonomous Mobile Systems

Xavier DÉFAGO
School of Information Science,
Japan Adv. Inst. of Science & Tech. (JAIST)

JAIST Japan Advanced Institute of Science and Technology, The 21st Century COE Program
Verifiable and Evolvable e-Society

1

Motivation

JAIST

2

Goal

Dependable Infrastructure for a Trustworthy e-Society

- **Dependable Infrastructure**
  - Mechanisms, methodologies for dependable infrastructures
- **Trustworthy e-Society**
  - Face new challenges

JAIST

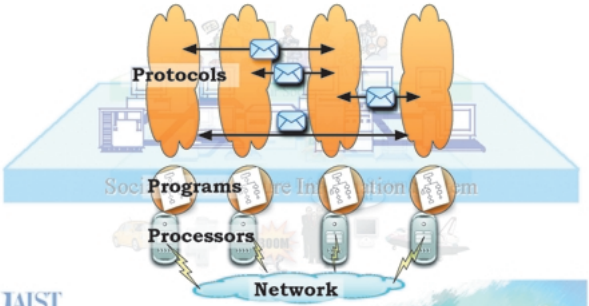
3

Our Research Area

JAIST

4

Our Research Area



JAIST

5

Outline

- Terminology
- Group Communication & Agreement
- Fault-Detection
- Autonomous Mobile Systems
- Concluding Remarks

JAIST

6

Terminology

- **System properties**
  - Safety vs. Liveness
- **Safety**
  - Never do "BAD" things.
  - *Ex., (vending mach.): coffee button & got smtg => get coffee*
- **Liveness**
  - Eventually do "GOOD" things.
  - *Ex., (vending mach.): any button => get smtg after a while*

JAIST

7

Fault-Tolerant Systems

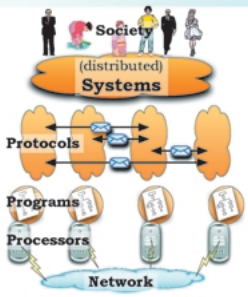
	No Faults	Faults	
	Safety & Liveness	Safety	Liveness
Ideal FT	○	○	○
Pragmatic FT	○	○	Probability 1
Fail-safe	○	○	×

JAIST

8

Challenges

- **Requirements**
  - Safety, liveness,...
- **Uncertainty**
  - Network delays
  - Faults
  - Load, users behavior
- **Challenges**
  - Hide uncertainty
  - Graceful degradation
  - Fail-safety

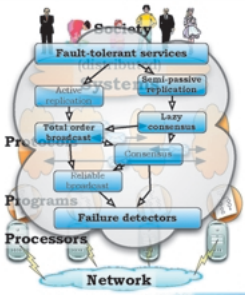


JAIST

9

Protocols: Agreement

- **Distributed Systems**
  - collection of **services**
  - need for **consistency**
  - masking faults, **replication**
- **Agreement**
  - central issue, many instances
    - group, leader
    - atomic actions
    - reconfiguration
- **Protocols**
  - resilient agreement protocols



JAIST

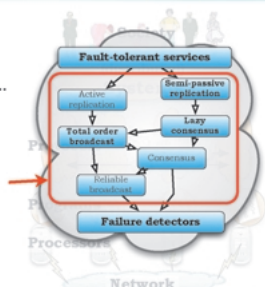
10

Group Communication & Agreement

11

Distributed Agreement

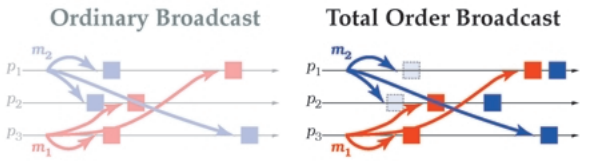
- **Situation**
  - Many instances
    - Leader, group, ordering,...
- **Tot. Order Bcast**
  - ... on **ordering**
- **Leader election**
  - ... on **leader**
- **Transactions**
  - ... on **commit / abort**
- **Consensus**
  - ... on **value**



JAIST

12

Total Order Broadcast



- **Total Order Broadcast**
  - Broadcast primitive
  - Hosts deliver **same sequence** of messages

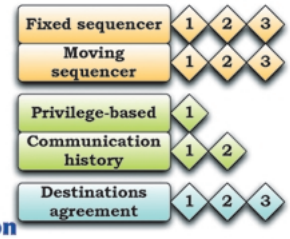
JAIST

13

13

Total Order Broadcast: Taxonomy

- **Survey [CSUR 04]**
  - 60 algorithms
- **Taxonomy**
  - 5 classes
  - 12 variants
- **Basis for comparison**

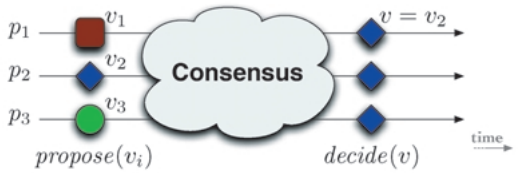


JAIST

14

14

Consensus



- **Definition**
  - Participants **propose value**
  - Agreement on **decision value**

JAIST

15

15

Fault-Detection

16

16

Failure Detection

- **Distrib. agreement & group comm.**
  - Fault-tolerant algorithms rely on failure detectors
- **Evaluation**
  - Performance influenced by failure detectors: detection time, mistakes
- **Requires**
  - Failure detectors

JAIST

17

17

Goal

Fault-Detection as
Generic Service

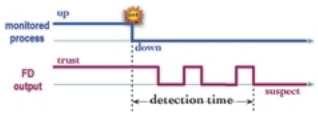
JAIST

18

18

QoS of Failure Detectors

- **Latency**
  - Detection time
  - *"How long to detect?"*
  - The shorter the better.

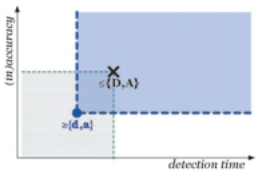


- **Accuracy**
  - Mistake rate
  - *"How often suspect?"*
  - The fewer the better.

JAIST

19

Requirements vs. Guarantees

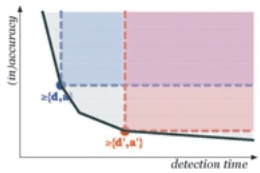


- **Application requirements**
  - ≤{D,A} : max. detect. time, max. mistakes
- **FD QoS**
  - ≥{d,a} : effect. detection time, effect. mistakes

JAIST

20

Parametric Failure Detector



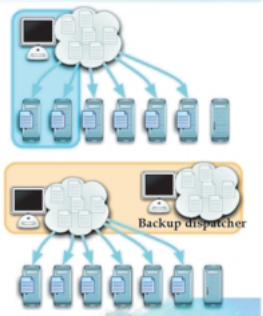
- **Parametric FD protocol**
  - Parameter value defines **FD instance**
  - Tradeoff: accuracy <-> detection latency
  - All possible instances define **QoS coverage**

JAIST

21

Different Patterns

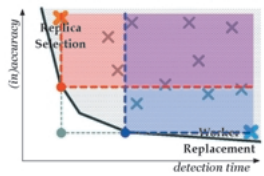
- **Dispatcher–Worker**
  - Action: release resources
  - Needs stability
  - => *conservative FD*
- **Dispatcher–replica**
  - Action: failover
  - Needs quick reaction
  - => *mid. aggressive FD*



JAIST

22

Simultaneous FD Instances



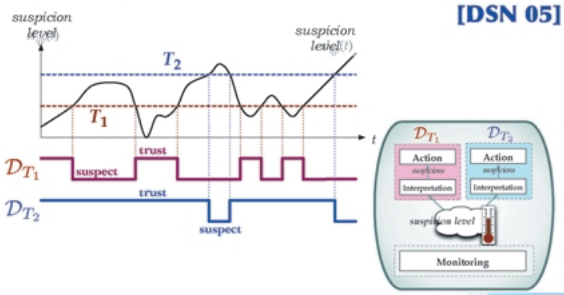
- **FD Instances**
  - Single instance not sufficient
  - But, no extra cost.
  - => Support for **multiple** instances

JAIST

23

Accrual Failure Detectors

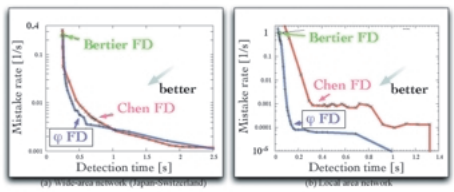
[DSN 05]



JAIST

24

φ FD: Performance Evaluation



- **Global network (left)**
  - similar to Chen
- **LAN (right)**
  - 10 times less mistakes than Chen

[SRDS 04]

JAIST

25

25

Autonomous Mobile Systems

26

26

Context & Motivation

- **Context**
  - Group of mobile robots
- **Objective**
  - Prevent robot collisions
- **Guidelines**
  - Decentralized
  - Asynchronous communication
  - Asynchronous positioning system
  - Isolate synchronous & RT assumptions

JAIST

27

27

Context

- **Equipment**
  - 4 Pioneer-3 robots
    - Laptop
    - Wireless (WiFi; bluetooth)
    - Sonar (180°, 6-7m)

- **Observation**
  - Ranges:
    - Sonar: 7m
    - Bluetooth: 10m
    - WiFi: 100m

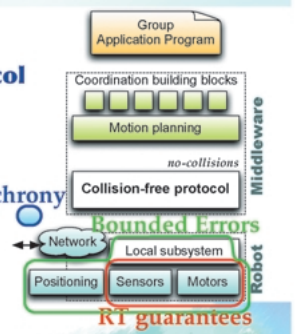
JAIST

28

28

Architecture

- **Collision-free protocol**
  - Ensure no-collision
  - Fail-safe behavior
- **Local subsystem**
  - Individ. robot movements
  - Detect inert obstacles
  - Use sonars



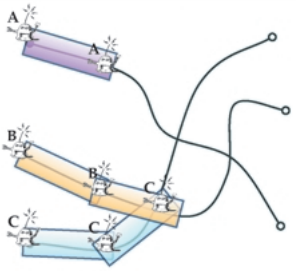
JAIST

29

29

Path Reservation

- **Robot knows**
  - **own** destination / path
  - **own** location
- **Does NOT know**
  - others' destinations
  - others' location
  - others' velocity
  - communication delays
- **Reservation**
  - *request*: request lock
  - *release*: release lock



JAIST

30

30

Two Models

[YCDW06]

	Model 1	Model 2
Comm. range	*Unlimited*	*within range D*
Group	Static	Dynamic
Group knowledge	Full system	Partial; within range D
Synch. assumpt.	◊S failure detector	Neighborhood discovery
Scalability	Low	Very high
Fault-tolerance	YES	not yet
Deadlocks	Detect locally	Detect within range D

JAIST

31

Concluding Remarks

32

Conclusion

- **Protocols**
  - Agreement issues
  - Scalability, evaluation
- **Means**
  - Fault detection
  - Evaluation, control
- **Environment**
  - Location awareness
  - Mobile systems

JAIST

33

Ongoing & Future Work

- **Agreement**
  - Scalability, QoS
  - Groups of people
- **Failure Detection**
  - Large-scale monitoring, experimentation
  - Use control theory; QoS stability
- **Mobile Systems**
  - Middleware platform: single system view
  - Hybrid systems: sensor networks & mobile nodes
  - Theory: minimal assumptions
  - Self-stabilizing, self-organizing protocols

JAIST

34

Questions? & Answers?

JAIST

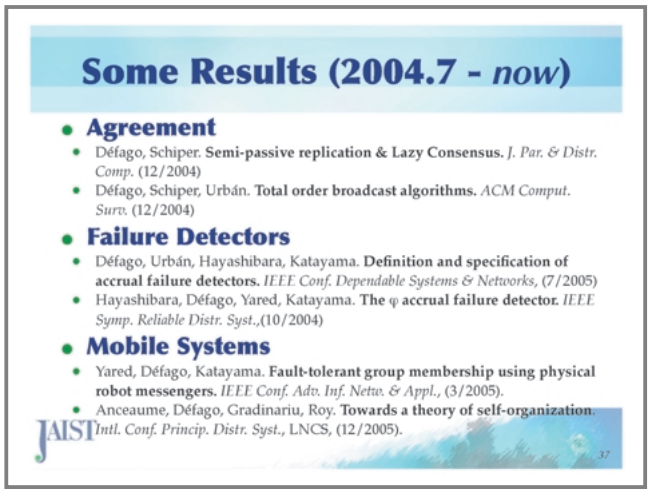
35

Collaborations

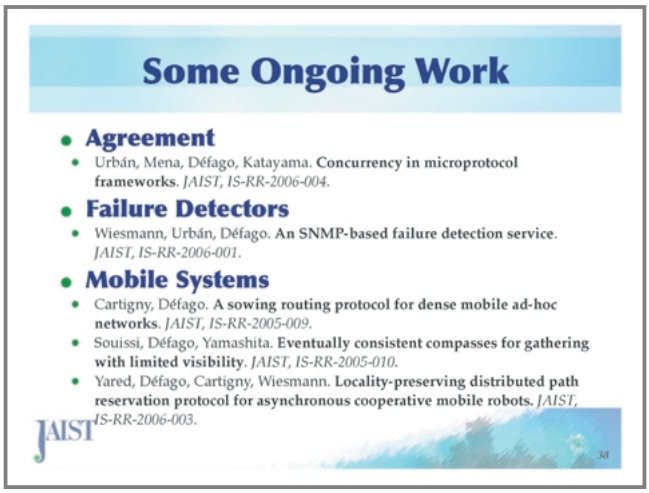
- **Agreement**
  - Swiss Federal Institute of Technology, Lausanne (EPFL)
- **Failure Detectors**
  - Tokyo Denki University
  - AT&T research (in discussions)
- **Mobile Systems**
  - JAIST, Chong lab.
  - Kyushu University
  - IRISA - Univ. Rennes, France

JAIST

36


Some Results (2004.7 - now)
Agreement
Défago, Schiper. Semi-passive replication & Lazy Consensus. J. Par. & Distr. Comp. (12/2004)
Défago, Schiper, Urbán. Total order broadcast algorithms. ACM Comput. Surv. (12/2004)
Failure Detectors
Défago, Urbán, Hayashibara, Katayama. Definition and specification of accrual failure detectors. IEEE Conf. Dependable Systems & Networks, (7/2005)
Hayashibara, Défago, Yared, Katayama. The φ accrual failure detector. IEEE Symp. Reliable Distr. Syst.,(10/2004)
Mobile Systems
Yared, Défago, Katayama. Fault-tolerant group membership using physical robot messengers. IEEE Conf. Adv. Inf. Netw. & Appl., (3/2005).
Anceaume, Défago, Gradinariu, Roy. Towards a theory of self-organization. Intl. Conf. Princip. Distr. Syst., LNCS, (12/2005).
JAIST
37

37


Some Ongoing Work
Agreement
Urbán, Mena, Défago, Katayama. Concurrency in microprotocol frameworks. JAIST, IS-RR-2006-004.
Failure Detectors
Wiesmann, Urbán, Défago. An SNMP-based failure detection service. JAIST, IS-RR-2006-001.
Mobile Systems
Cartigny, Défago. A sowing routing protocol for dense mobile ad-hoc networks. JAIST, IS-RR-2005-009.
Souissi, Défago, Yamashita. Eventually consistent compasses for gathering with limited visibility. JAIST, IS-RR-2005-010.
Yared, Défago, Cartigny, Wiesmann. Locality-preserving distributed path reservation protocol for asynchronous cooperative mobile robots. JAIST, IS-RR-2006-003.
JAIST
38

38


Other Research Activities
Invited Talks
IFIP WG 10.4 meeting, summer 2005
IFIP WG 10.4 meeting, winter 2006
etc...
Program Committees
IEEE Symp. Reliable Distrib. Systems, 2004
IEEE Intl. Conf. Dependable Systems & Networks, 2005
IEEE Intl. Conf. Distrib. Comput. Systems, 2006
etc...
JAIST
39

39

インターネットシミュレータによる電子社会の安心性検証

篠田　陽一
北陸先端科学技術大学院大学 情報科学センター

JAIST 21世紀COEシンポジウム2006

インターネットシミュレータによる電子社会の安心性検証

情報科学センター　篠田 陽一
情報科学研究科　丹 康雄

1

StarBEDインターネットシミュレータ

- 北陸IT研究開発支援センター（通称StarBED）として2002年度に開所。
- *汎用インターネットシミュレーション環境* として利用者による検証作業用に提供するとともに、経験の蓄積や支援環境の整備を行なってきた。



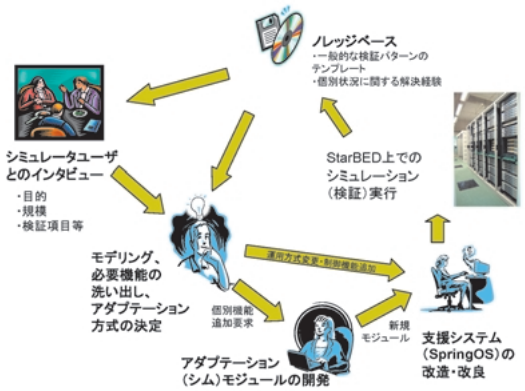
2

StarBEDの生い立ち

- 動機
  - ネットワーク関連の各種研究開発において必須である、実証実験用テストベッド構築に要する時間とコストを大幅に削減したい。
- 汎用インターネットシミュレータ として構想・設計・構築・運用
- ミッションプロファイル
  - 従来は実証的に行なうことが非現実的であった、大規模で複雑なネットワークシステムの性能予測・解析・評価を可能にする。
    - 実証的な検証を妨げていた要因
      - 検証用システムの構築
        - ハードウェアリソース
        - 時間制約(設計・調達・構築)
      - 検証実施ノウハウの欠如

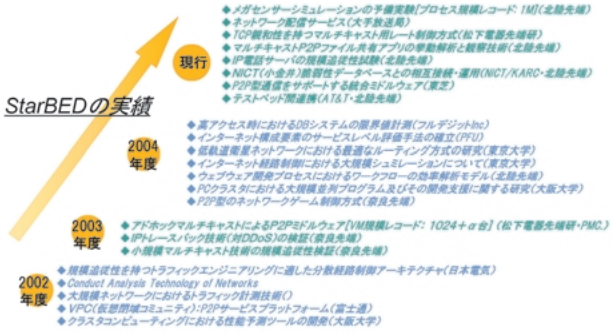
3

StarBEDでの基本アクティビティ



4

ユーザ検証実績（抜粋）



5

SpringOS: StarBEDのオペレーティングシステム

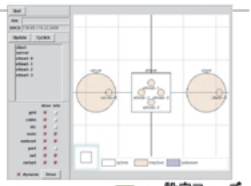
- 高度に連携したモジュールから構成される、洗練されたオペレーティングシステムが（当初）計画されたが・・・
- そのようなシステムは作り難く、さらに使いにくいことが経験からわかった。
- 現在のSpringOSは、必要に応じて組み合わせることのできるコア機能コンポーネントの集合になっている。
  - リソースマネージャ（ノード、VLAN、、、）
  - ノードソフトウェアローダ（OS + ユーザーランドアプリケーション）
  - ノードディスク操作エージェントとコマンダー
  - ネットワークトポロジの自動設定
  - 実験スクリプトの並列分散評価機構
  - 進行状況のビジュアライザ
  - ノードヘルスチェッカ
  - オンメモリOSジェネレータ

6

SpringOSの動作イメージ

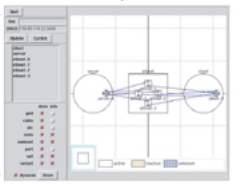
環境記述 （トポロジ部）

```
nodeset client class c num 1
nodeset server class s num 1
netset ethnet class e num 4

attach server.netif["lan0"] ethnet[0]
attach server.netif["lan1"] ethnet[1]
attach server.netif["lan2"] ethnet[2]
attach server.netif["lan3"] ethnet[3]

attach client.netif["lan0"] ethnet[0]
attach client.netif["lan1"] ethnet[1]
attach client.netif["lan2"] ethnet[2]
attach client.netif["lan3"] ethnet[3]
```



設定フェーズ

実行フェーズ



検証実行記述

リモートプログラム実行と同期操作の集合として記述される

7

StarBED自身に関する研究成果

- シミュレーション・エミュレーションのためのモデリング技法の蓄積
  - シミュレーション・エミュレーションでは、ターゲットシステムのモデリング技術（抽象化手段）は共通基盤となる技術である。これについて、既存のパッケージを適用するだけで済むシステムと、特殊な要求を持つシステムの切り分け方や、後者のシステムではサポート用サブシステムの開発を通して知識の蓄積と整備を行なった。
- 支援ツール群・支援環境の整備
  - 利用者とのモデリングのコンサルテーションを通して、支援ツール群やそれらを統合して制御するための支援環境(SpringOS)を開発した。
- 現実的な環境での、性能・精度などの実証実験を行なうためのフレームワーク確立
  - モデリング技法の蓄積と支援支援環境の整備を通して、インターネット指向システムの実証実験を行なうためのフレームワークを確立した。

8

StarBED2: シミュレーション対象の拡大

目的

●従来のインターネット技術のみのシミュレータから、各種ネットワーク（モバイル、センサーなど）が結合した新世代ネットワークアーキテクチャの評価・検証が可能な高度・大規模シミュレータ環境を構築

各種ネットワークが結合した新世代ネットワークのシミュレーションが可能な環境の構築

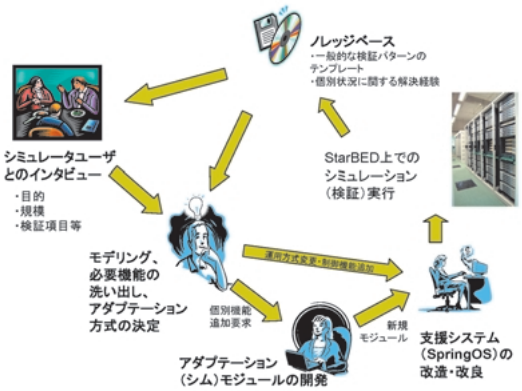
最大5万台規模のルーター、最大100万個規模のセンサネットワーク等、各種ネットワークが融合

大規模シミュレーション環境を構築

従来(StarBED)からあるインターネット技術のシミュレーション環境

9

StarBEDでの基本アクティビティ

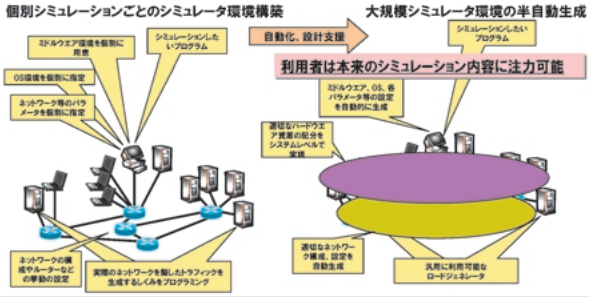


10

StarBED2: シミュレーション支援環境

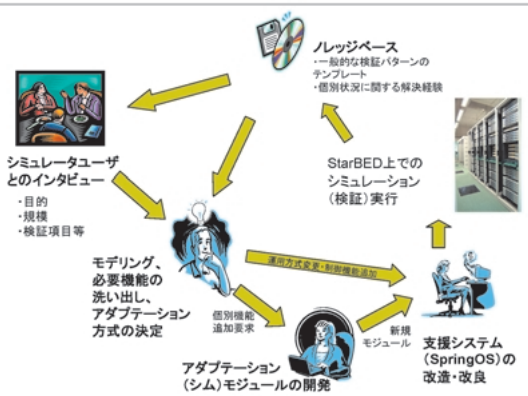
目的

●シミュレーションに当たって必要な各種設定を、可能な限り自動化・半自動化するとともに、各種ネットワークシステム・アプリケーションのモデル化技術を開発することにより、利用者が本来のシミュレーション内容に注力できるよう、シミュレーション環境の高度化を行う。



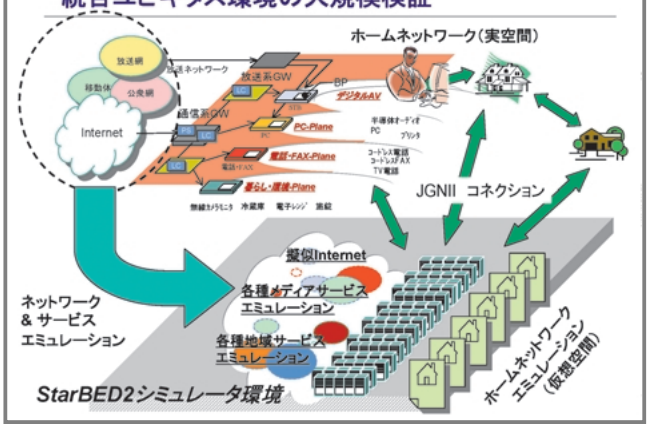
11

StarBEDでの基本アクティビティ



12

StarBED2 ユビキタスシステムシミュレータによる統合ユビキタス環境の大規模検証



13

StarBED: Other activities

- 複数テストベッドの連携動作
  - 類似テストベッドの結合による実験規模拡大(スケールブースト)
    - 規模面で、より現実的な実証実験を可能に。
  - テストベッドシステムの拡大適用(シームレススケーラビリティ)
    - 実験室規模の実験から現実規模の実験への容易な移行。
  - 異種テストベッドの役割分担による結合(ファンクションブースト)
    - 機能面で、より現実的な環境での研究開発を可能に。
    - 新しい機能を持ったテストベッドの創出。
- Planet-Lab(Priceton/Intel/HP)との協調 / クラスタコンピューティングシステムのパートタイムデプロイメント
- 他の(実践的)シミュレーションシステムの取り込み

14