JAIST-COE/AIST-CVS シンポジウム：形式検証技術―現状と安心電子社会への適用

JAIST 情報科学研究科

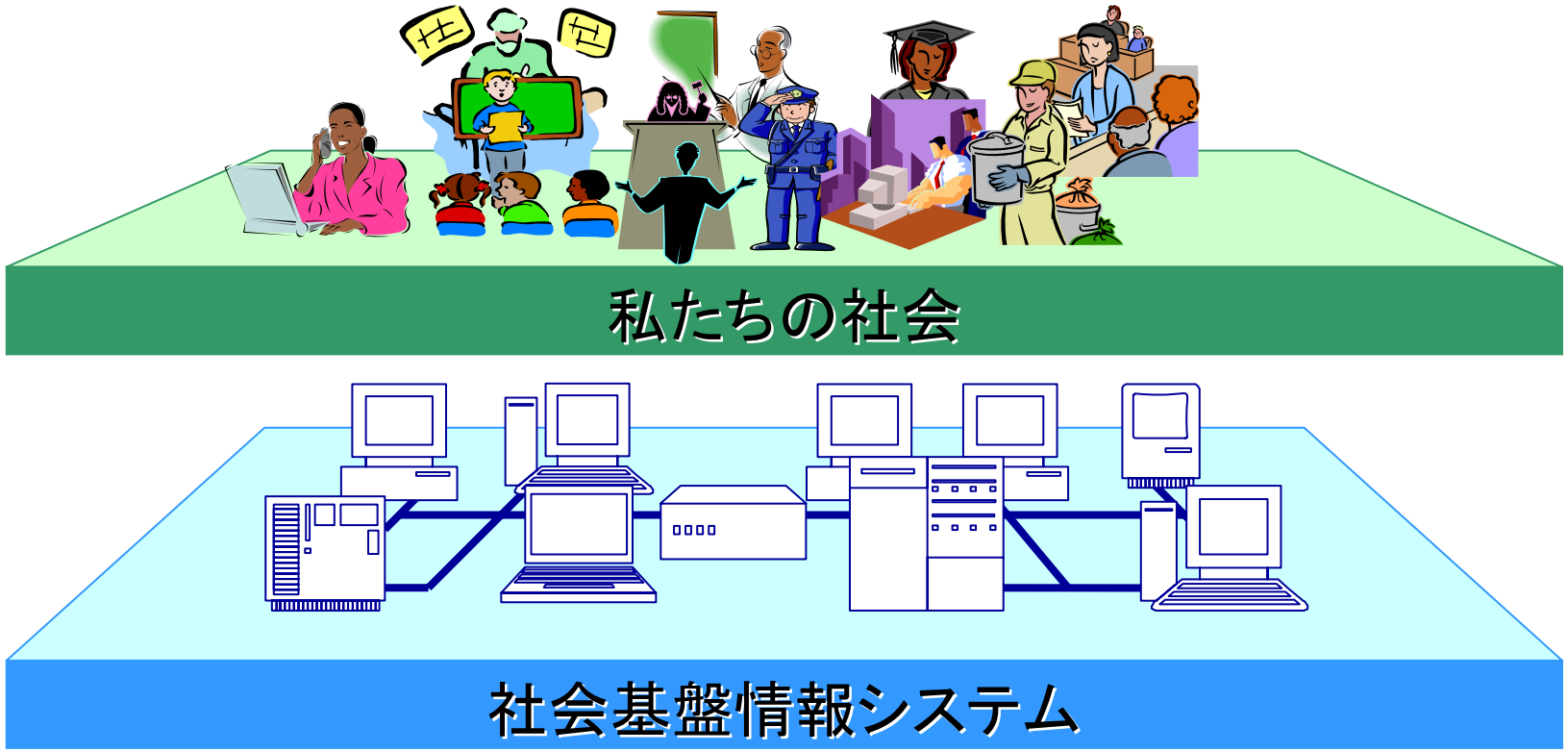
片山卓也

JAIST 北陸先端科学技術大学院大学
21世紀COEプログラム 検証進化可能電子社会
Verifiable and Evolvable e-Society

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 –

電子社会

- 情報システム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



電子社会の安心性要件

1.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？

2.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？）

3.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？

4.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？

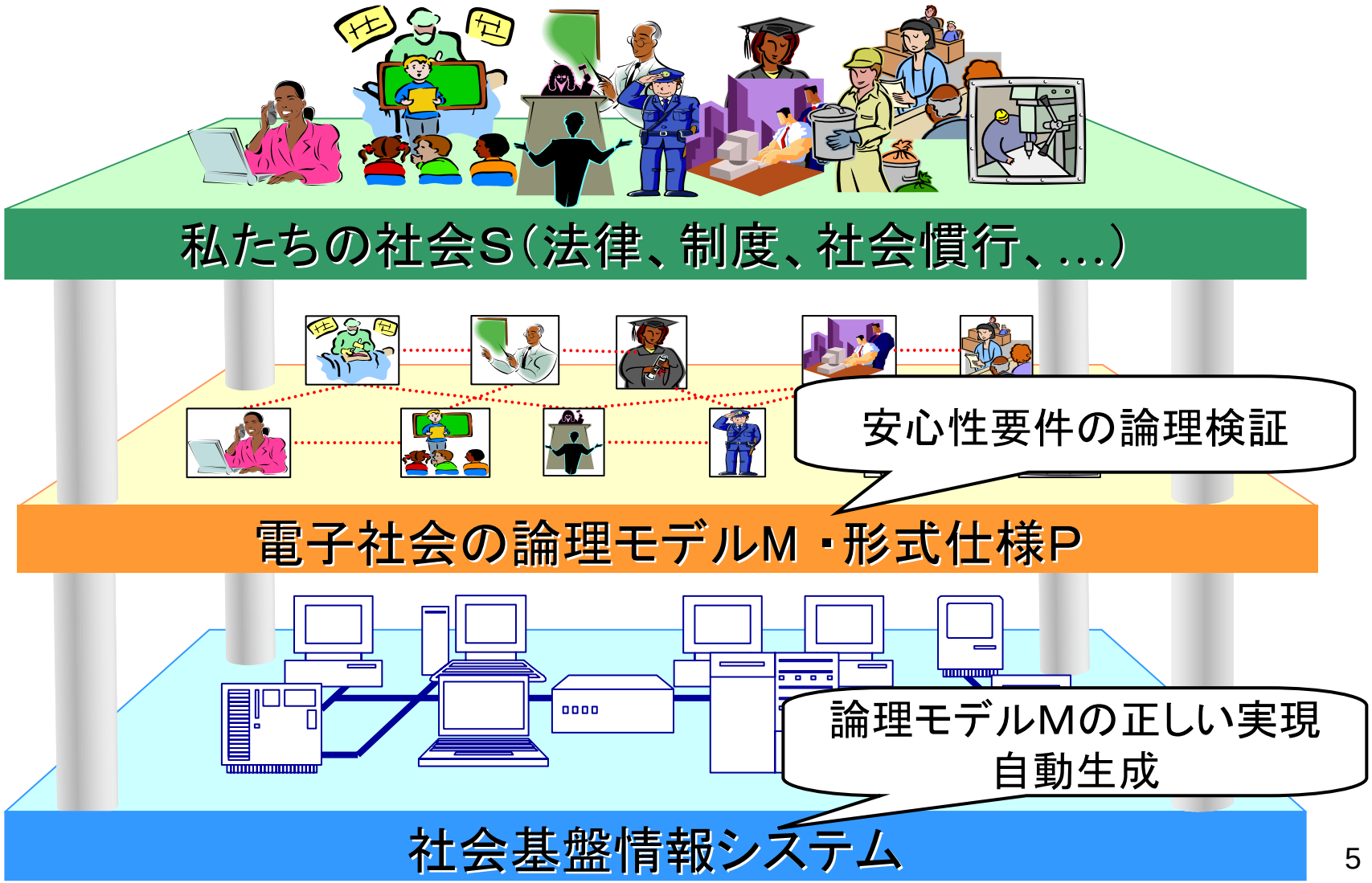
5.耐故障性

事故や故障があっても
機能し続けるか？

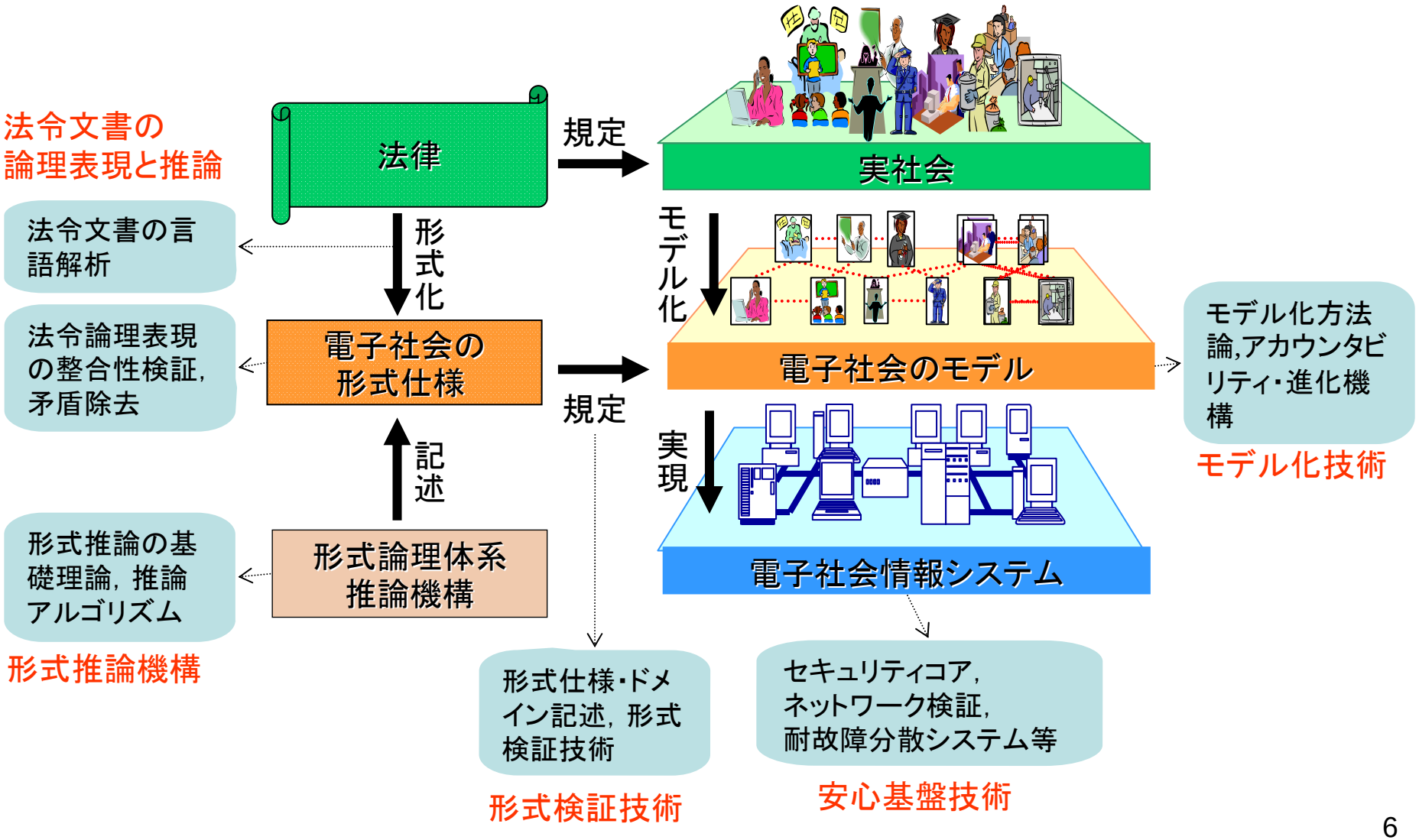
6. 高信頼情報基盤

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？

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

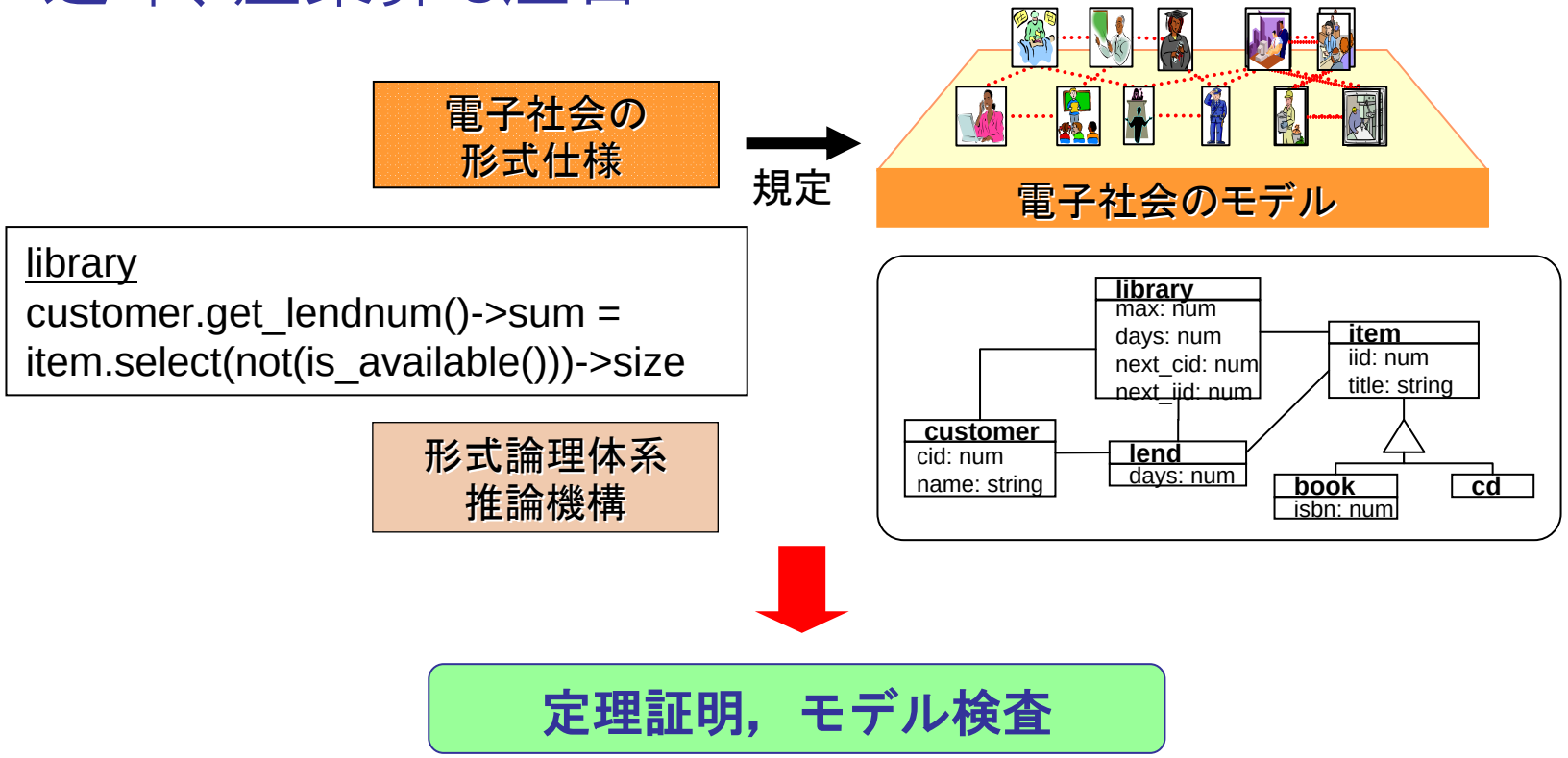


研究課題の設定


法令文書の
論理表現と推論
法律
規定
実社会
法令文書の言
語解析
形
式
化
モデル化
法令論理表現
の整合性検証，
矛盾除去
電子社会の
形式仕様
規定
電子社会のモデル
モデル化方法
論,アカウンタビ
リティ・進化機
構
モデル化技術
記
述
実
現
形式推論の基
礎理論，推論
アルゴリズム
形式論理体系
推論機構
電子社会情報システム
形式推論機構
形式仕様・ドメ
イン記述，形式
検証技術
セキュリティコア，
ネットワーク検証，
耐故障分散システム等
形式検証技術
安心基盤技術

形式検証技術

- 情報システムがその仕様を満たすことを、定理証明などの数学的方法を用いて確立する技術
- 近年、産業界も注目



COEにおける形式検証研究の取り組み

- 形式検証技術はCOEの基本課題
  - 形式推論機構の理論
    - 小野、小川、Vestergaard
  - 形式仕様記述、定理証明技術による検証
    - 二木、緒方、片山
  - モデル検査技術と組み込みシステムの検証
    - 青木、岸
  - ハイブリッド系の検証
    - 平石
- 産総研システム検証研究センターとの協調
  - ワークショップの共同開催