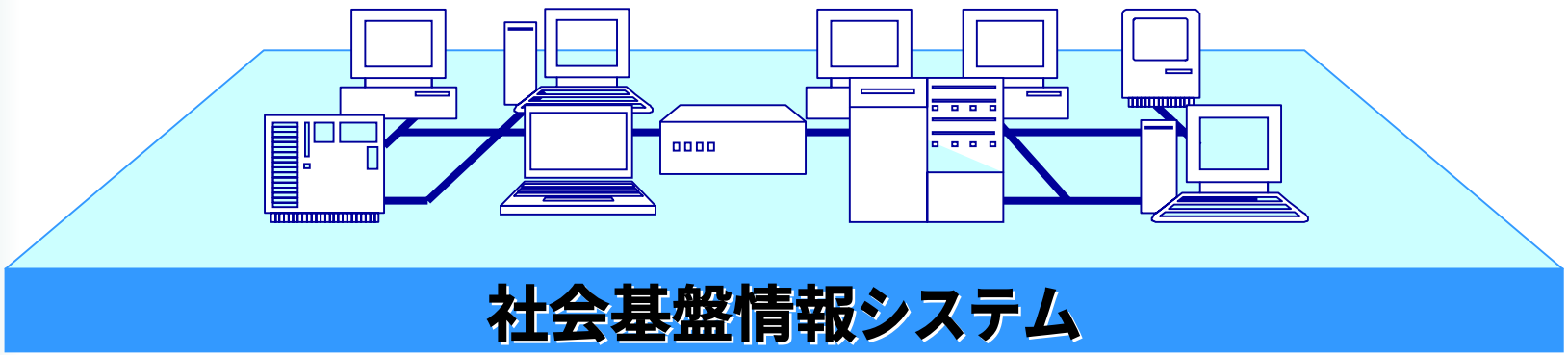
検証進化可能電子社会
- 情報科学による安心電子社会の実現 -

北陸先端科学技術大学院大学
情報科学研究科
片山卓也

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



安心な情報システム

- 安心　Trustworthy
  - 広辞苑
    - 心配・不安がなくて，心が安らぐこと．また，安らかなこと．
  - ジーニアス和英
    - relief（安堵感）,ease(気楽さ), rest(安楽), security(安全，無事)
    - trustworthy(信用・信頼できる，当てになる)
- 安心な情報システム
  - 信頼できる，当てになる情報システム
  - 間違った処理をしない，壊れない，セキュリティが高い
- 正当性，アカウンタビリティ，セキュリティ，耐故障性，進化性

安心な電子社会

正当性

電子社会の機能や構造が法律や制度と整合しているか？

- 社会システムの仕様：法律，法規
- 電子社会：社会システム仕様の実現
  - 電子社会の機能や構造は，法律や法規を正しいく実現しているか？
  - 税金の計算は正しいか？

安心な電子社会

アカウンタビリティ

電子社会の機能や構造についての質問や疑問に
対して説明可能か？

- 電子社会の仕様である法律や法規に照らして，質問に答え得るようにシステムは作られているか？
  - 私の税金は，なぜそうなのか？
  - その処理は男女差別をしていなか？
- 人間によるシステム理解の困難性，悪意のある為政者，技術者

安心な電子社会

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？

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るか？

- 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

安心な電子社会

進化性

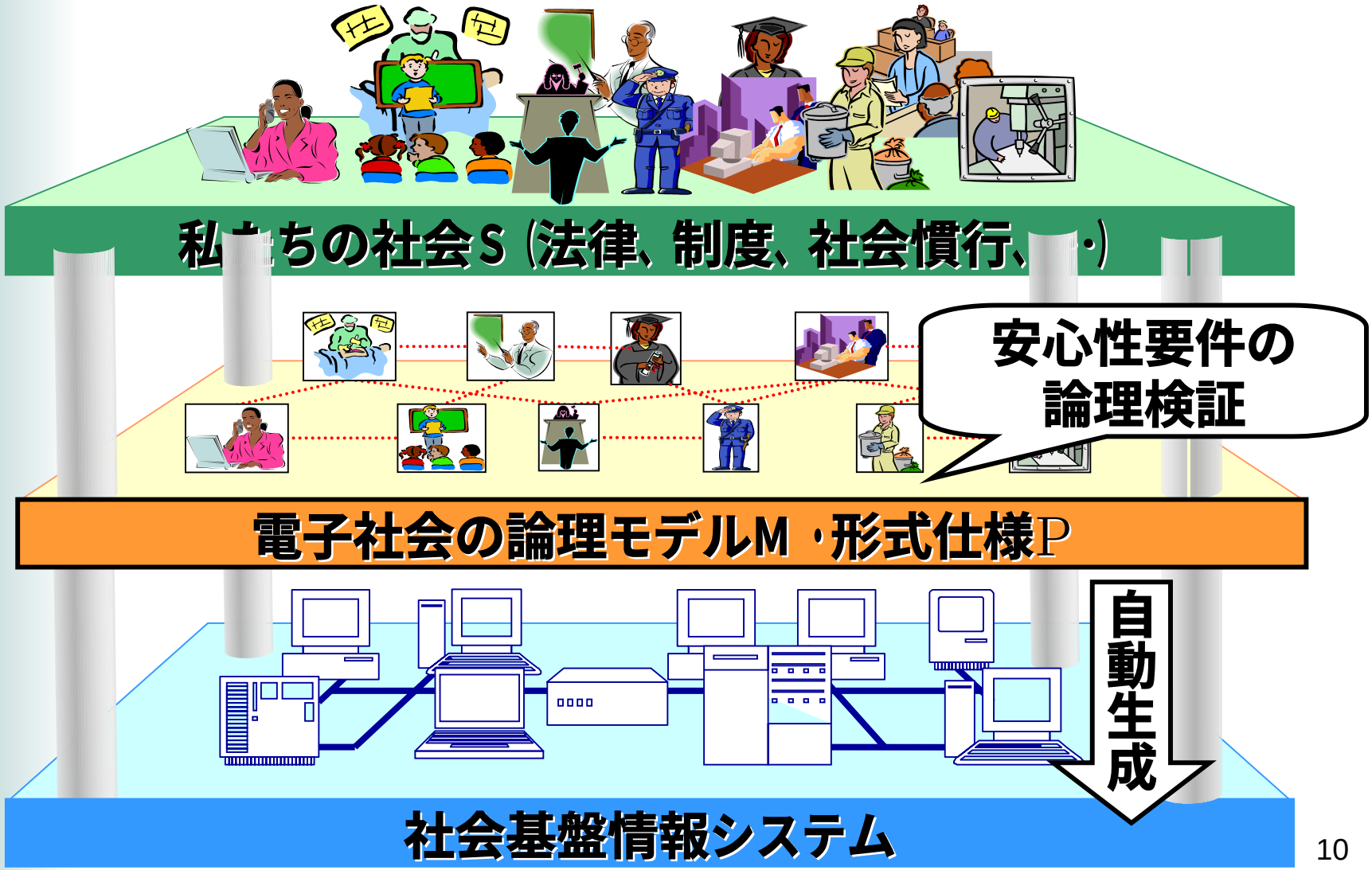
社会情勢や環境の変化に適応して、
電子社会を適切に変更出来るか？

- 進化性がないと社会の停滞を招く
- 情報システムの最も困難な問題

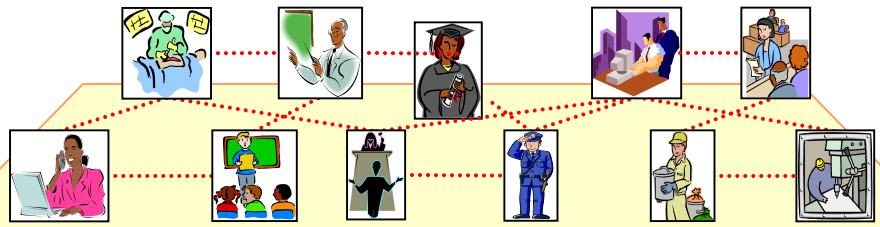
情報科学は，安心な電子社会の実現にどのように寄与できるか？

- 安心な情報システム　Dependable Information Systemの構築には，情報科学は有効であった．
  - 安心性
    - 正しく動作する
    - 故障しない，故障に強い
    - 不正なアクセスや 侵入に強い
  - 安心性のための技術
    - システム検証技術：定理証明システム，モデル検査，形式仕様記述
    - 耐故障技術：複製化技術，チェックポイント・ロールバック技術，原子ブロードキャスト
    - セキュリティ技術：暗号理論，認証
- これらの技術は，安心な電子社会の構築に有効か，他に必要な技術がいるか？
  - 安心性情報技術を社会モデルに適用

安心性要件を満たす電子社会の実現法



電子社会の論理検証



電子社会の形式仕様P・論理モデルM

安心性要件

正当性

アカウンタビリティ

セキュリティ

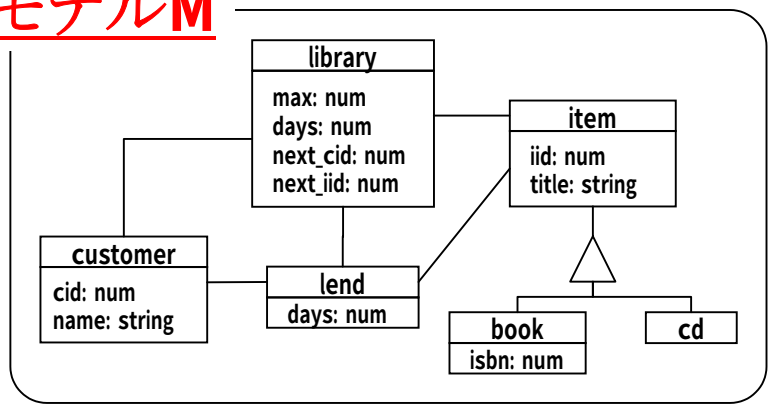
耐故障性

進化可能性

形式仕様P

```
library
customer.get_lendnum()->sum =
item.select(not(is_available()))->size
```

論理モデルM



論理検証 M models P

定理証明システム
シミュレーション実行

キーとなる技術1
モデル駆動アーキテクチャMDA

- 電子社会システム自身のモデル化
  - 抽象度を高め，検証や進化を容易にする．
    情報システム⇒電子社会
  - 非本質的な詳細の排除による検証コストの削減
    - 従来の検証コストは，プログラムレベルの詳細度を相手にしていたために非常に高くなっていた．
  - 情報システムは，電子社会モデルから自動合成
    - 現在のソフトウェア工学のMDAは，
      情報システムのモデル⇒プログラム
  - 必要な技術
    - 電子社会自身の仕様記述，モデル化

キーとなる技術2
検証技術，自動生成

- 研究成果は積み上げられている．
  - 定理証明システム，モデル検査ツール，検証方法論
  - 特に，ヨーロッパで顕著
  - 日本では，…
- コストは高いが，高信頼なシステムの構築に効果的
- 現実問題への適用
  - 多くの先進事例（軍事，宇宙）はあるが，民需システムへの適用はこれから
  - （特にモデル検査法の）組込みシステムへの適用への関心が高まっている．
- コート量が多くなく，高い抽象化レベルで設計された対象なら，定理証明，モデル検査ともに，実用システムについても適用可能
- 自動生成
  - モデルが明確に構成されていれば可能
  - ビジネスシステムに関するMDAツール

「検証進化可能電子社会」

- 「検証進化可能電子社会」
  ー情報科学による安心電子社会の実現ー
- 21世紀COEプログラム，H16年度採択
- 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

拠点形成の目的ー研究ー

- 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
  - 電子社会の検証･進化の実証

拠点形成の目的ー人材養成ー

- 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

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情報科学を適用

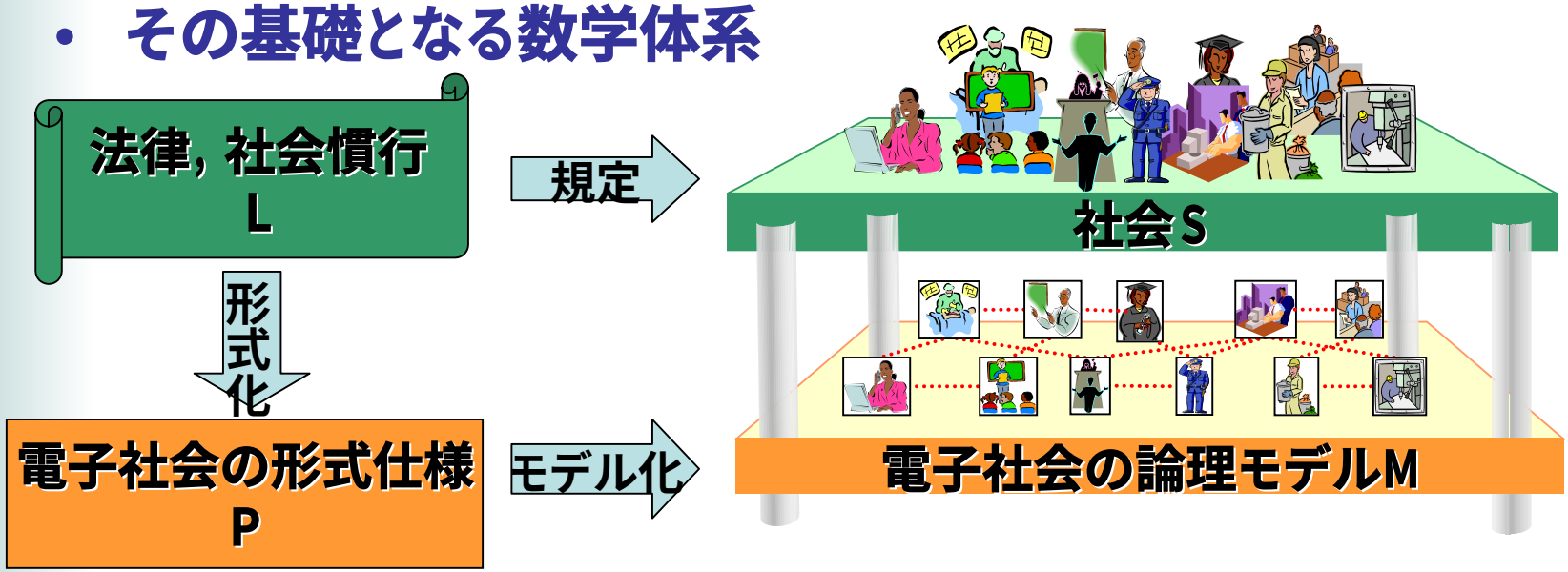
これまでの電子政府・社会研究における情報技術の適用

- 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

検証進化可能電子社会研究課題

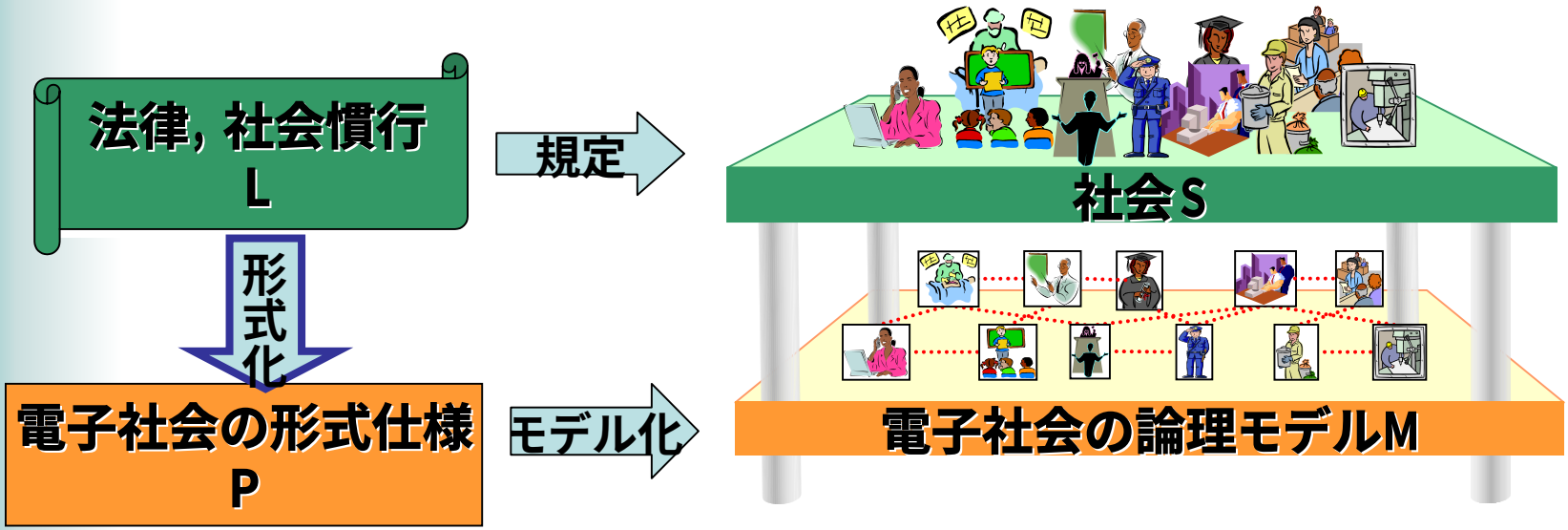
電子社会の形式的仕様記述体系

- 形式体系・論理F：電子社会中の個人や組織，その役割・権限・機能などが記述可能
- Fの証明方法論，定理証明システム・実現用メタ言語ML
- その基礎となる数学体系



形式論理体系F
Fの定理証明系

電子社会の法推論と言語処理

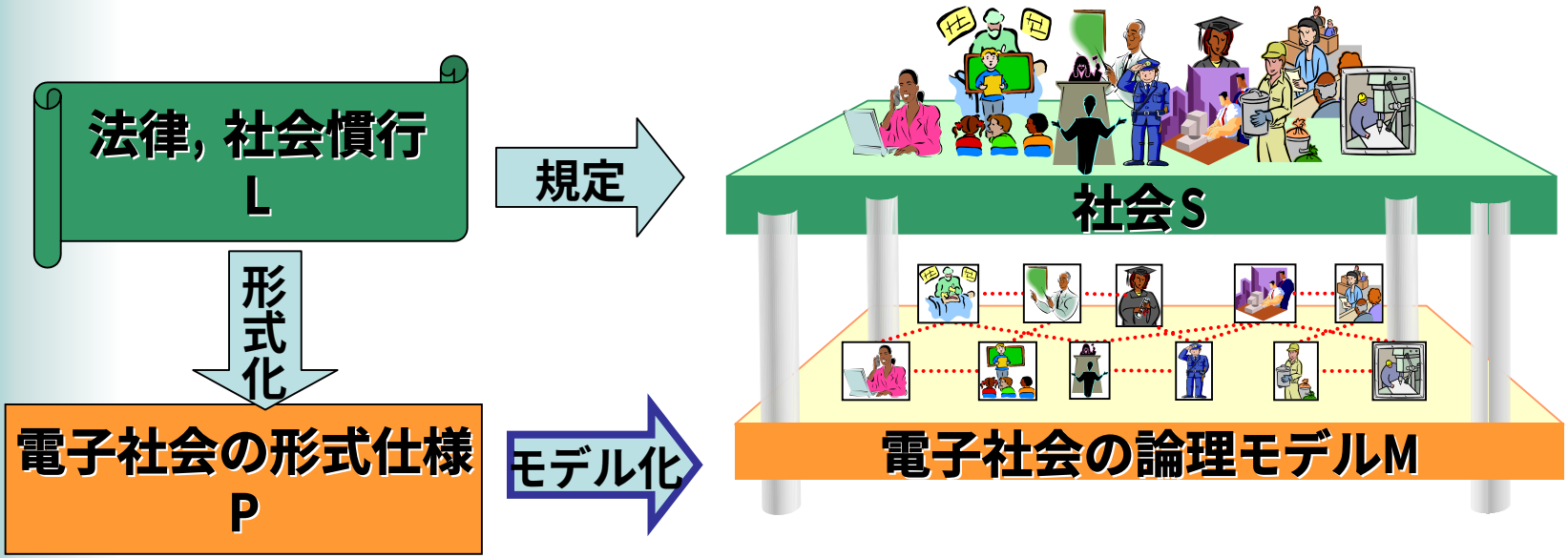


- 法律文書Lから論理表現Pをどのように作るか？
  - 自然言語処理＋手仕事
  - 法律文書に近い論理体系の構築
- Pは矛盾していないか？　矛盾の除去
  - 定理証明技術による自動処理
- Pについての質問Q
  - 推論 P|-Q として実行
  - 推論結果をいかに “普通”の人に伝えるか？

- 法律体系の准無矛盾性の検証.ppt
- HWshimazu041118.ppt

電子社会の正当性検証

- 電子社会の機能やサービスの正当性の検証



- M ⊢ P の検証
  - 従来のソフトウェア検証技術の適用．具体的には，Mの与え方による．
  - オブジェクト指向モデル，ワークフローモデル
- 大きなコード量によって実問題への適用が阻まれていたソフトウェア検証技術が，電子社会モデルに対しては，成功する可能性が高い．

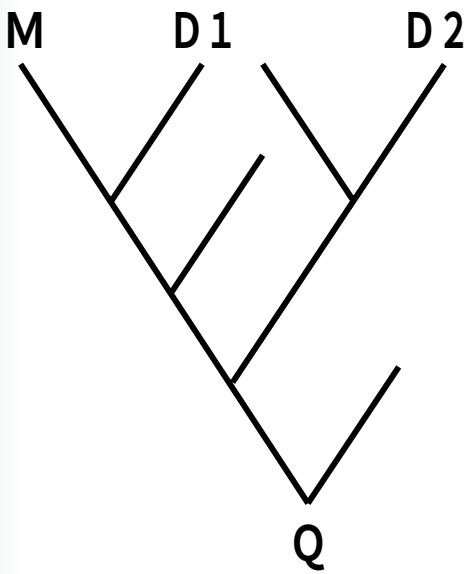
電子社会のアカウンタビリティ

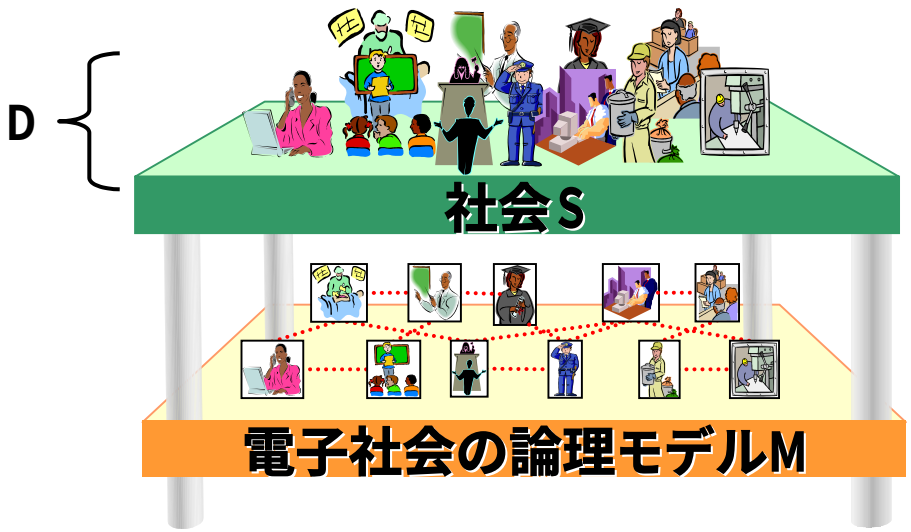
モデルMに関する質問Qに答える.

- M and D ⊢ Q, ただし, D：社会に関する関連知識
- M and D ⊢ Q の証明過程から, 説明文を作り出す.
- Mと質問Qの距離が遠い場合は, 機械的処理は困難

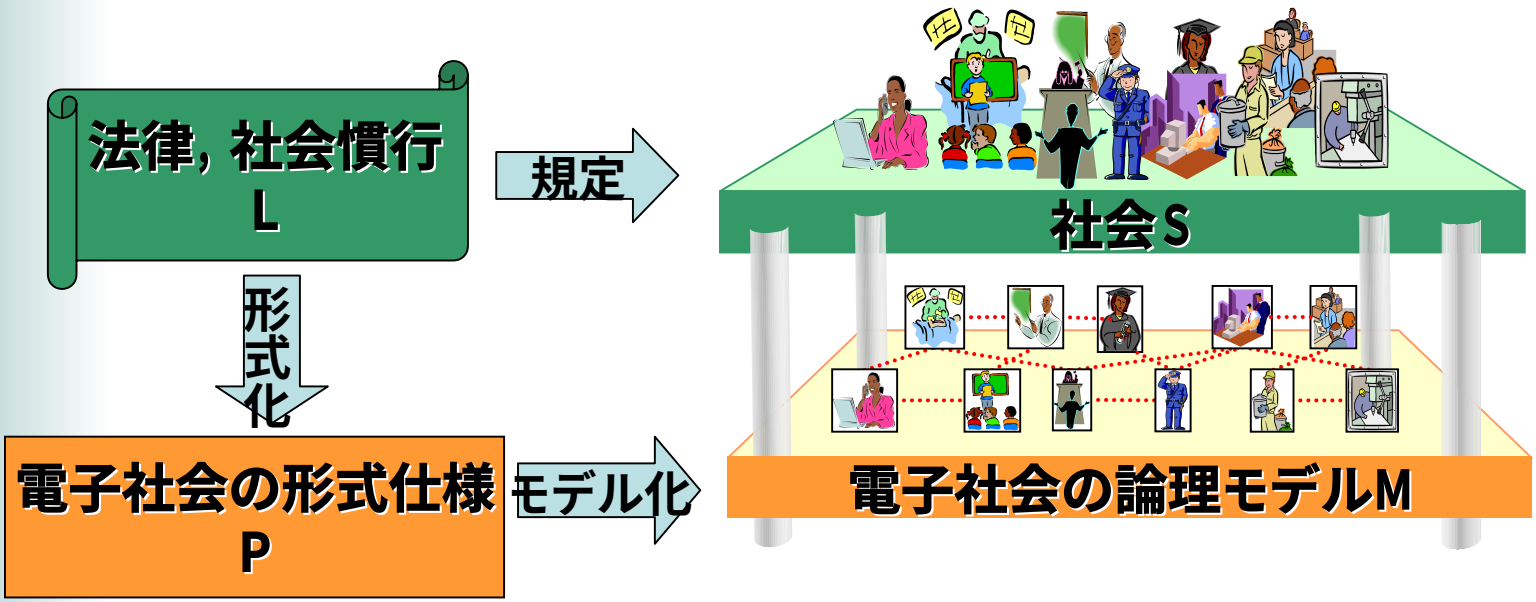
“その処理は, 憲法に違反してないか？”

- 全てがブラックボックスになってしまう電子社会では基本的
- これまでにほとんど研究されていない



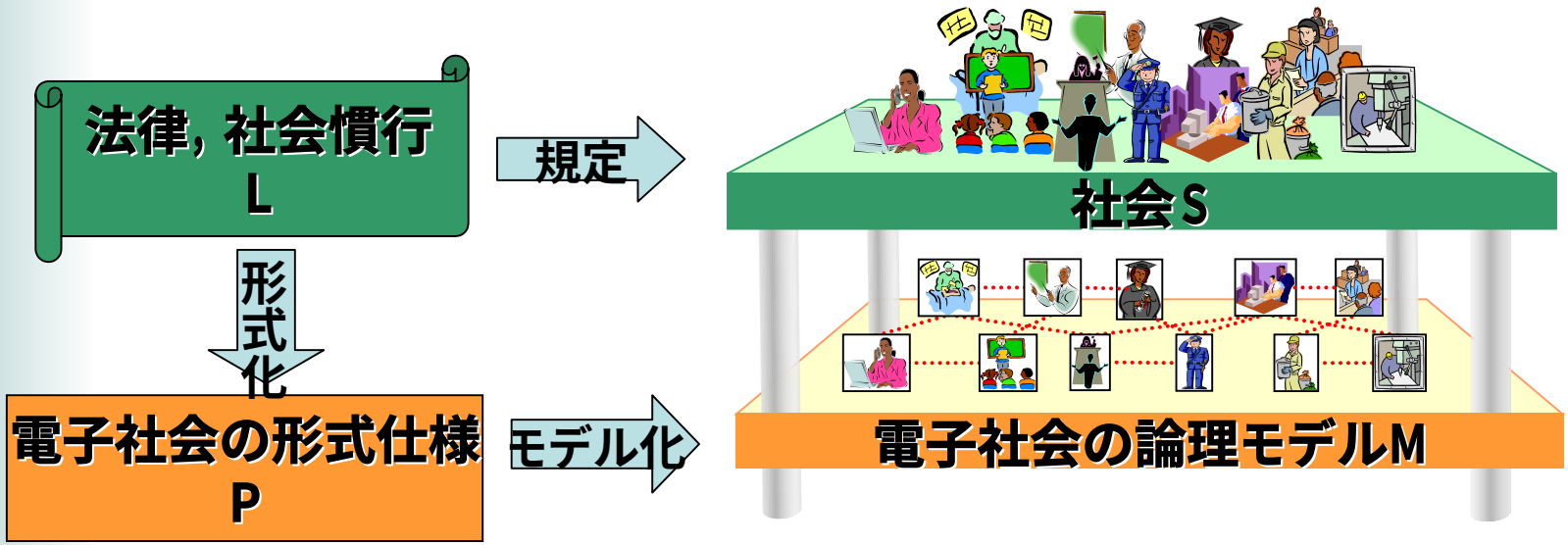


電子社会のセキュリティ



- Mのなかでは，データの漏洩や不正なアクセスは起きないか？
- プライバシーは保てるか
- それらをどのように証明できるか？
- 電子社会と情報セキュリティ.ppt

電子社会の耐故障性



- M中の個人や組織が動作をできなくても，Mはサービスを続行できるように作られているか？
  - 電子社会モデルに，分散システムの耐故障メカニズムを適用
    - メンバーシップ，コンセンサス，アトミックブロードキャスト
    - 冗長性：複製，チェックポイント・ロールバック
  - 計算機，ネットワークシステムとが違うところはどこか？
  - coe_FT.ppt

電子社会の安心性要件検証方式，ツール

- 定理証明やモデル検査による検証
  - すでに多くのシステムが開発されており，基本的にはそれらを利用．
  - COE04小川 (1).ppt
  - 社会システム固有の問題の取り込み方法
- エージェント技術による電子社会モデルのシミュレータによる電子社会の論理検証
  - 実際に，モデルを動作させることにより，法律や規則の不備などを発見するのに有効

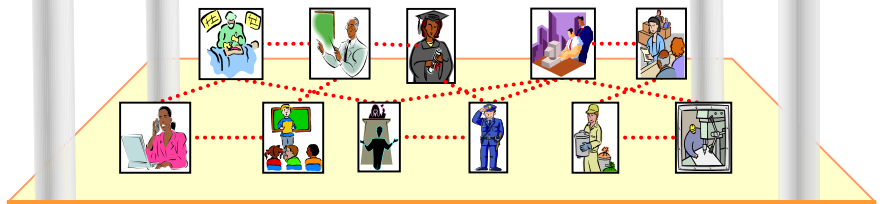
法律，社会慣行
L

規定

形式化

電子社会の形式仕様
P

モデル化



オブジェクト
システム
オブジェクト指向技術.ppt

ワークフロー
システム
workflow一平石.ppt

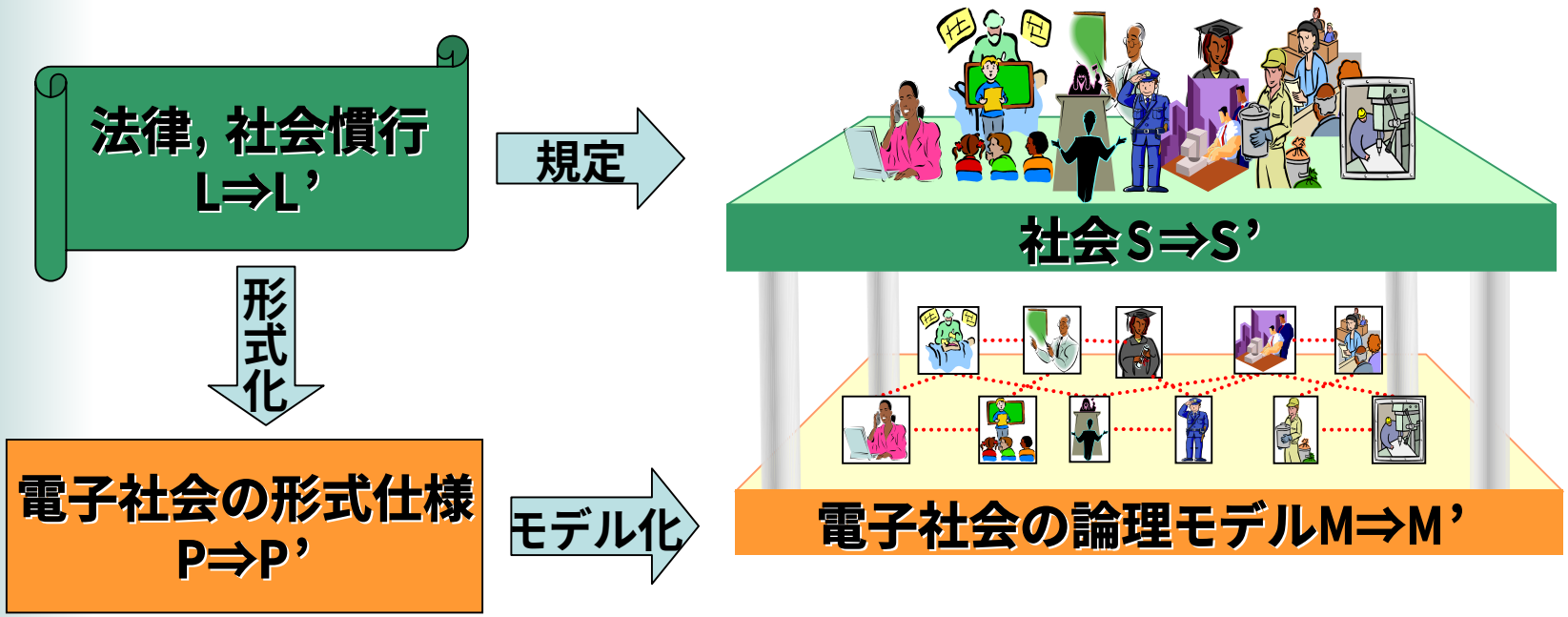
ネットワーク
エージェント
システム
Mobile Agents (Shen).ppt

StarBedインターネット
シミュレータ (NICT)

電子社会シミュレータ

- モデルMの正しさのテスト
- Mの動作のモデル検査
- Mの性能解析，数学モデル
- 耐故障解析

電子社会の進化機構



- 変化 P⇒P’において，P’に導入される矛盾の検出，除去，法推論処理
- P⇒P’に対応して，モデルの変更 M⇒M’ をどのように行うか？
  - 発展ドメイン理論，オントロジー，アスペクト

発展ドメイン理論.ppt

電子社会の検証進化の実証実験

- 地方自治体業務，企業システムを対象にした検証，シミュレーション
  - 富山県庁業務
  - NTTデータ社内システム