学位報告 4

報告番号	※　乙　第　　号

主　論　文　の　要　旨

論文題目　Formal Specification and Verification of Anonymity and Privacy
（匿名性とプライバシの数理的仕様記述と検証）

氏　　名　真野健

論 文 内 容 の 要 旨

本論文では，匿名性とプライバシの数理的仕様記述と検証について述べる．情報通信技術の発達により，ネットワークを介して個人情報/プライバシ情報をやりとりする機会は増えている．もちろん，関連法規の整備等により不要な収集や保持は避けられる傾向にあるが，それが本当に必要な状況では，匿名性やプライバシ保護が適切になされていることを確かめることが重要となる．情報システムにおいて匿名性とプライバシを検証するための数理的技法は，その有効な技術として期待されている．

匿名性・プライバシのための数理的技法には，大きく分けて 2 つのアプローチがある．ひとつは状態遷移モデルの研究にもとづくもの，もうひとつはマルチエージェントシステムと知識論理の研究にもとづくものである．

実際に数理的検証を行っている研究のほとんどは，前者の状態遷移モデルにもとづいている．状態遷移モデルでは模倣による証明技法がよく研究されており，これが実際の検証に有用だからである．一方，仕様の記述は基本的に動作の等価性を用いており，匿名性・プライバシの微妙な性質が表現できていないケースがある．たとえば実用的な投票プロトコルで，投票の棄権が想定される場合などである．

一方，知識論理は表現力の高さを特徴とし，それを行かしてさまざまな匿名性・プライバシ仕様を記述する研究がなされている．しかし，検証のための方法論は十分研究されていない．これら 2 つのアプローチを組み合わせることで，匿名性・プライバシの，柔軟な仕様記述と強力な検証を可能とする手法を実現したい．

そこで，本論文の第 2，3，4 章では，知識論理で匿名性/プライバシ仕様を記述し，それを状態遷移モデルの模倣証明技法によって検証するという方法論を提示する．第 2 章では，知識論理による匿名性・プライバシの定式化方法，第 3 章ではそれらのための模倣証明技法を提示する．また第 4 章では，当手法の適用可能性を確認するためのケーススタディとして，実用的な電子投票プロトコルの匿名性とプライバシの数理的検証を行う．さらに，第 5，6 章では，第 2 章で示した知識論理による匿名性・プライバシの数理的定式化における考え方を，2 つの方向に拡張する．第 5 章では，匿名性・プライバシのように情報隠蔽に関する性質だけでなく顕名性・アイデンティティなど情報公開に関する性質へ適用し，さらに第 6 章では，法的なプライバシ概念との比較検討へ適用する．

以下，各章ごとに要旨を説明する．
第 1 章は，イントロダクションである．本論文の背景，動機，関連研究，本論文のアプローチ，構成について述べる．
第 2 章では，本論文で用いる知識論理体系を説明する．知識論理体系は，単なる命題の真偽だけでなく，エージェント（行為者）が“～を知っている”“～を知らない”“～かもしれないと思う”といった知識に関する主張を表現するための体系であり，エージェント i の知識を表現する Ki という演算子を備える．知識論理のモデルとして，本論文では Halpern らによるマルチエージェントシステムの数理的なモデル（run and system framework）を用いる．
Halpern らはまた，匿名性を知識論理によって定式化する研究を行っている．そこでは，匿名性を記述するための基本述語として，主語と述語の関係を抽象的に表現する式 θ(i, a)（エージェント i がアクション a をした，あるいは i が属性 a を持っている，を表す）が用いられている．この基本述語を用いて，“そのアクションを，誰が行ったか分からない”という匿名性のさまざまなバリエーションを柔軟に記述し分けられることが，この定式化の特長である．
この研究にもとづき，本章では知識論理を用いて役割交換可能性（role interchangeability）を定義する．その意味は，“エージェント i が アクション a を，i’ が a’ を行ったとき，実は i が a’ を，i’ が a を行ったかもしれないと思う（ので，どちらが本当か分からない）”である．役割交換可能性自体は，匿名性の必要条件でも十分条件でもない．しかし簡単な付加的条件を仮定することで，そこから匿名を導出できる（定理 2.2.7，定理 2.2.9，系 2.2.10）．
さらに，プライバシを定式化する方法を示す．その特徴は，プライバシを匿名性と対称的な性質ととらえていることである．匿名性が“そのアクションを，誰が行ったか分からない”ことであるのに対し，プライバシを“そのエージェントが，何を行ったか分からない”という性質としてとらえ，知識論理式で定式化する．そのとき，匿名性とプライバシは対称的（これはある種の双対性ととらえることができる）なので，匿名性と対称的なしかたで，役割交換可能性と付加的条件からプライバシを導出することができる（定理 2.3.3，系 2.3.4）．
第 3 章では，役割交換可能性を模倣証明技法によって検証する方法を提示する．まず，マルチエージェントシステムと状態遷移モデルの対応関係として，強互換性（strong compatibility）を定義する．直観的には，状態遷移モデルの各トレースが，マルチエージェントシステムのどれかの run（実行系列）の

- 観測可能なアクション
- θ(i,a) の成立

を忠実に反映しているとき，そのマルチエージェントシステムは状態遷移モデルに対し強互換であるという．
個々のアクションの観測可能性は，暗号などによる情報隠蔽を反映して，アクションからアクションへの関数として定義される．さらに，模倣関係を表現する役割交換関数が定義される．エージェント i，i’ とアクション a，a’ に関する役割交換関数とは，トレースからトレースへの関数であって，任意のトレースとそれを役割交換関数で写像したトレースとの間に，

- 観測可能なアクションについて識別不能
- i と i’ の，a，a’ に関する役割が逆

という性質が成り立つものである．このとき，以下の定理が導かれる：

マルチエージェントシステムにおける役割交換可能性の成立と，それが強互換となる状態遷移モデルにおける役割交換関数族の存在は同値である（定理 3.2.2）．

第 2，3 章で得られた知見を総合すると，マルチエージェントシステムにおける匿名性・プライバシを検証するための，以下のような 2 段階からなる方法が得られる：

1. 状態遷移モデルの模倣証明技法を用いて，役割交換関数族の存在を証明する．それによって，互換なマルチエージェントシステムにおける役割交換可能性が証明される．
2. 役割交換可能性と付加的条件とから，匿名性，プライバシを導出する．

第 4 章ではこの方法を用いて，実用的な電子投票プロトコル F00 の匿名性とプライバシを検証する．F00 は柔軟かつ効率的な電子投票プロトコルであり，これをもとに発展させたプロトコルが多数考案されている．一般に，実用的な電子投票プロトコルはさまざまな暗号プリミティブを含むので，数理的検証のよい題材とみなされている．F00 を I/O オートマトンと呼ばれる記述方法で状態遷移モデルとして記述し，それをもとに上記 2 段階の検証を実行することで，F00 の匿名性とプライバシを数理的に検証する．

第 5 章では，プライバシに関わる情報隠蔽性および情報公開性についての分類学を提案している．ここでは匿名性，プライバシとともに顕名性，アイデンティティが考察の対称となっている．顕名性は，その行為を行ったのが誰かという情報を公開するのに対し，アイデンティティは，その行為者が行ったアクションは何かを公開する性質である．本章では，それらの性質を数理的に定義し，相互の論理的な関係を明らかにする．さらに，個々の匿名性・プライバシと，顕名性・アイデンティティが両立可能（モデルを持つ）か否かを解析する．また，プライバシに関わる既存の用語集と，提案する分類学との対応について述べる．

第 6 章は，法的な文脈への適用について述べる．比較のための実例として，宴のあと事件判決を取り上げる．同判決は，私法上のプライバシ権に関する事件において広く判例として用いられている．本章ではこの判決を法的なプライバシ概念の定義とみなし，第 2 章で数理的に定式化したプライバシと比較する．宴のあと事件判決で要件の一部となっている同定可能性に関して，法的プライバシと数理的プライバシの間の相違を指摘し，その相違の意味および同定可能性の要件としての妥当性を，現在の技術的文脈に照らしつつ検討する．その結果，同定可能性を緩和するあらたな要件として自己情報性を提案する．

第 7 章では，まとめと今後の課題を述べる．付録では，第 4 章で示した補題や定理の証明の詳細を述べる．