別紙１－１

論文審査の結果の要旨および担当者

報告番号	※ 乙　　第　　号

氏　　名　　真野　健

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）

論文審査担当者

主　査　　名古屋大学教授　　坂部　俊樹

名古屋大学教授　　外山　勝彦

名古屋大学教授　　結縁　祥治

別紙１－２

論文審査の結果の要旨

真野健君提出の論文「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）」は、情報システムの匿名性とプライバシの数理的な仕様記述と検証に関する一連の研究をまとめたものであり、全体は 8 章から構成される。

第 1 章は序論であり、本研究の背景として、情報通信技術の発展にともない情報システムにおける個人情報の保護（プライバシ）が重要な問題となる現状について説明し、情報隠蔽に関する数理的検証の必要性について述べている。また、数理的検証のためには、匿名性とプライバシを知識論理体系で定式化し仕様記述するための方法論が重要であることを説明している。さらに、実問題の検証に関して多くの実績のある状態遷移モデルの模倣証明技法と、上記仕様記述法とを結びつけることの有用性について述べている。

第 2 章は、知識論理体系を用いた匿名性とプライバシの仕様記述の方法について述べている。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とそれを用いた匿名性の定式化に関する研究をもとに、プライバシやその他関連する性質を定式化・記述するための方法論を提示している。具体的には、匿名性・プライバシの知識論理による仕様記述と状態遷移モデルの模倣証明技法とを結びつけるために、新たに役割交換可能性を定義し、役割交換可能性が成り立つことを前提として、匿名性・プライバシの導出方法を示している。

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している。まず、エージェントアクション集合が役割交換可能性をもつことと、対応する状態遷移モデルに対して役割交換関数族が存在することとが互いに必要十分条件であることを示している。役割交換関数は、状態遷移モデルのトレースからトレースへの関数であり、任意のトレースを、それと識別不能でかつ役割が逆となるトレースに写像するものである。これにより、知識論理で記述した匿名性・プライバシを模倣証明技法により検証できることを示している。

第 4 章では、前章で得られた方法を、実用的な電子投票プロトコル FOO に対して適用するケーススタディについて述べている。FOO はさまざまな暗号プリミティブを用いた実用的セキュリティプロトコルであり、匿名性とプライバシの数理的検証の題材として広く用いられているが、有権者が棄権する可能性を考慮した数理的検証は従来行われていなかった。前章の検証手法によって、それが可能となることを示している。

第 5 章では、第 2 章で提示された匿名性・プライバシの数理的定式化と同様の考え方を、顕名性やアイデンティティなど情報公開に関する性質へと拡張することで、それらの性質の分類法を提示している。数理的に定式化されたさまざまな性質の間の論理的含意関係や両立可能性に関する基本的な結果を示している。また、プライバシに関わる既存の用語集と提案する分類法とを比較検討することで、前者が網羅しきれていない概念の存在を示している。

第 6 章は、プライバシの数理的定式化の、法的な文脈への適用について述べている。私法上

のプライバシ権に関する最重要判例である宴のあと事件判決との比較から、同判例の同定可能性に関する問題点を指摘し、その解決として自己情報性という概念を新たに提示している。また、自己情報性と数理的プライバシ概念の間に緊密な対応関係があることを示している。

第 7 章は結論であり、本論文の成果をまとめるとともに、今後の課題について述べている。また第 8 章は付録であり、第 4 章で示した補題や定理の証明の詳細を述べている。

以上のように本論文は、情報システムの匿名性やプライバシを数理的に検証する技術に関する課題に対して有効な技術・知見を提示している。いずれも、学術的な新規性に加えて、実用性も高いものであり、情報科学の学術上・技術上の寄与が大きい。よって、本論文の提出者真野健君は、博士（情報科学）の学位を受けるのに十分な資格があるものと判定した。