（ 続紙 1 ）

京都大学	博 士（ 理 学 ）	氏名	南　規楽
論文題目	Trace Equivalence and Epistemic Logic to Express Security Properties （セキュリティ特性を表現するためのトレース等価と認識論理）		

（論文内容の要旨）

暗号通信や電子投票システムなどの漏洩してはならない機密情報を扱うプロトコルについて、それらが意図されたとおりの安全性をみたしていることを数学的に証明するセキュリティ検証は、情報通信システムの設計と運用の大前提となる基礎的な問題であり、今日の社会のインフラストラクチャの安全性向上に密接に結びつく、極めて重要性の高い研究課題である。しかしながら、セキュリティ検証をおこなうための理論的枠組みについては、これまでに数多くの提案があるものの、その妥当性や正確さまで含めて確立されているものは決して多くはない。本論文では、セキュリティ検証をおこなう枠組みとして、プロセス代数のひとつである応用π計算と、知識を扱うことができる論理体系である認識論理を用いるアプローチを提案し、その理論的基礎と応用に向けた妥当性について論じている。

プロセス代数（またはプロセス計算）とは、複数の主体（プロセス）が相互に通信を行い計算を進めていく過程を抽象化した数学モデルであり、様々な情報通信プロトコルの定式化や検証に用いられてきた。本論文では、セキュリティ検証に適したプロセス代数としてAbadiらが導入した応用π計算（applied π-calculus）を、セキュリティプロトコルを記述するために用いる。応用π計算は、特に暗号プロトコルを自然に表現することが可能であるようにデザインされている。

プロセス代数の理論の礎となるのが、ふたつのプロセスを同一視する基準を定める等価性の概念である。議論の目的に応じて、古くより様々な等価性の概念が論じられており、代表的なものとして、外部から観測できるプロセスの挙動をもっとも精密に捉えた等価性である双模倣関係、またプロセスの動作の痕跡（トレース）をもとに定まるトレース等価性などが挙げられる。セキュリティ検証のために適した等価性がどれであるかは議論の余地があるが、本論文では、応用π計算によるセキュリティ検証においては、トレース等価性が、非適応的な攻撃者が存在する状況下において適切な等価性であることを、以下に述べるトレース等価性の合同性をもとに示していく。

プロセスの等価性が合同性を持つとは、システム中のプロセスを等価な別のプロセスで置き換えても、得られた新しいシステムはもとのシステムと等価である、という性質である。合同性は、システム全体の性質を、システムを構成する小さなプロセスたちの性質から合成して得ること（合成的推論）を可能にする、システム検証において非常に重要な概念である。応用π計算の前身であるMilnerらのπ計算では、トレース等価性が合同性を持たないことがよく知られている。しかし、応用π計算においては、π計算とは異なる変数のインスタンス化の仕組みを採用しているため、実は合同性が成り立つ。これは本論文の主要な成果のひとつであり、これまでに知られていなかった新しい知見である。その証明のために、束縛名のスコープの変化を追跡しやすい並行標準形という概念を導入し、合同性の完全な証明を与えている。

プロセス代数のプロセスの性質を捉えるために、様々な様相論理が提案されている。本論文では、応用π計算のための様相論理として、認識論理を採用する。この様相論理では、「命題φが成り立つことを攻撃者が知っている」ことをあらわす様相論

理式Ｋφを用いる。本論文のふたつ目の主要な結果として、この認識論理における論理的等価性が、応用π計算におけるトレース等価性と同値であることを示した。トレース等価性の合同性とあわせると、この認識論理を用いて合成的な推論を行うことが可能となる。応用として、この論理を用いて秘密性や役割交換可能性を定義し、プロセスへの操作でそれらが保たれるか否か、およびトレース等価との関係を述べている。

（続紙　２　）

（論文審査の結果の要旨）

プロセス計算を用いたセキュリティ検証の研究は２０年以上前から行われており、本研究の対象となった応用π計算もその文脈で提案され、多くの研究者によって研究されてきた。しかし、ふたつのプロセスが同一視できるかどうかというプロセス等価性の問題は、プロセス計算の理論の中心的なテーマであるにも関わらず、セキュリティ検証の観点から適切な等価性を追求するというアプローチは、これまでほとんど行われてこなかった。本研究は、先行研究にしばしばみられる思い込みを排し、一定の（非適応的な攻撃者が存在するという）仮定の下では、多くの場面で無批判に用いられている双模倣関係よりも、トレース等価性のほうがセキュリティ検証のためにより適切であることを、理論的根拠を示して論じている。特に、応用π計算におけるトレース等価性が合同関係であることは、本研究によってはじめて示された。この合同性は、π計算では成立しないことが広く知られており、それゆえに専門家たちも見過ごしていた意外な発見であり、先行研究に見られた偏見を打破する重要な貢献である。さらに、合同性により知識論理を用いた見通しの良い合成的な証明が可能となり、本論文によってトレース等価性を用いることの有用性が明らかにされたと言える。なお、合同性の証明は決して自明なものではなく、そのために新たな標準形の概念を導入するなど、様々な工夫がなされ、長大ながら見通しの良いものとなっていることにも評価すべき点である。

もちろん、本論文とは異なる仮定の下でのセキュリティ検証については今後の研究を待たなくてはならないし、他のプロセス等価性の有用性についても更なる議論が必要と考えられる。しかし、プロセス等価性という基礎的な問題意識に立脚して従来の常識・偏見を覆す成果を得たこと、また対応する論理体系を与え原理的にはこのアプローチにより有用なセキュリティ検証が可能であることを説得力を持って示していることは、高く評価できる。今後、本研究の成果が、今後の当分野の発展に大きな影響を及ぼすことが大いに期待できる。

よって、本論文は博士（理学）の学位論文として価値あるものと認める。また、令和４年１月２６日、論文内容とそれに関連した事項について試問を行った結果、合格と認めた。

要旨公表可能日：　　年　　月　　日以降