様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１８　日現在

機関番号：　１２１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６３３００７６

研究課題名（和文）知識の形成過程の分析による暗号プロトコルの安全性検証法に関する研究

研究課題名（英文）A Study on Security Verification Method of Cryptographic Protocols by Analysis of Knowledge Formation Process

研究代表者

長谷部　浩二（Hasebe, Koji）

筑波大学・システム情報系・准教授

研究者番号：８０４７００４５

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究は，知識論理を用いて，プロトコルの実行における参加者間での知識の形成過程を分析することにより，プロトコルの安全性を示す検証法の確立を目指して行われた．
本研究では，命題論理をもとにした動的知識論理による定式化と，動的様相を排した一階述語論理による定式化を行った．その結果，論理体系の表現力や体系の複雑さに関する問題が明らかとなった．しかしながら，その成果は分散システムにおけるいくつかのプロトコルの検証法などへの応用の可能性を示唆するものであった．また，プロトコルの実行に関していくつかの仮定を置くことで，検証法として有用な体系に近づくことができたと考えられる．

研究成果の概要（英文）：This research aimed at establishing a verification method showing the safety of cryptographic protocols by analyzing the formation process of knowledge among participants in the execution of protocols using epistemic logic.
In this research, formalization with the Propositional Dynamic Epistemic Logic and formalization with First-Order Predicate Epistemic Logic excluding dynamic modal operators were conducted. As a result, problems concerning the expressiveness of the logical system and the complexity of the system were clarified. However, the results suggested the possibility of application to verification methods of some protocols in distributed systems. Moreover, by putting some assumptions about the execution of the protocol, it seems that we could obtain a system useful as a verification method.

研究分野：　数理的技法

キーワード：　仕様記述・検証　数理的技法　暗号プロトコル　安全性検証　論理推論体系

１．研究開始当初の背景

数理的技法による暗号プロトコルの安全性検証法は，これまで BAN 論理を端緒に数多く提案されてきた．BAN 論理は，知識論理と呼ばれる様相論理の派生体系の一種であり，プロトコルの実行過程におけるネットワーク参加者の知識に関する推論を定式化したものである．BAN 論理による検証の基本的なアイデアは，「プロトコルの実行過程において，参加者の知識がどのように形成されるとプロトコルは安全であると言えるのか」という知識と安全性の関係に注目するというものである．BAN 論理は，簡潔な証明によって安全性の説明ができることから，多くの後継の論理を生み出す元となった．しかし一方で，これらの論理はいずれもメッセージの送受信の順序が記述できないといった表現力の弱さがあり，十分な検証能力を持たなかった．

その後 1990 年代に入ると，プロトコルの実行結果そのものを分析する手法が数多く現れ，BAN 論理で発見できなかったプロトコルの脆弱性が次々と発見されるようになった．すなわちこの時期以降，研究の主要な関心は，「各参加者がプロトコルを正しく実行すると，プロトコルの目的（情報の秘匿や認証の成立など）が常に実現されるのか」という問題に移っていったと言える．

こうした経緯から，BAN 論理に代わる論理推論を用いた安全性検証法としては，Protocol Composition Logic（PCL）や，研究代表者らによって PCL を単純化した Basic Protocol Logic などが挙げられるが，知識論理を用いたものはあまり例がない．知識と安全性との関係を分析するという BAN 論理のアイデアは，それ自体に問題があった訳ではないものの，その有用性が十分に考察されないまま今日に至っている．特に，「参加者 *A* がプロトコルに従っていることを参加者 *B* が知っている，ということを参加者 *A* が知っている」といった，知識の共有に関する命題の成立と安全性との間の一般的な関係については，未だ解明されていない．

一方，知識論理の分野においては，Gerbrandy らによって提案された動的知識論理（Dynamic epistemic logic）の研究が精力的に行われてきた．動的知識論理の基本的なアイデアは，従来の知識論理に対して，新たにプロセス（命令もしくは動作の実行列）を記述するための動的様相オペレータを導入するというものである．これにより，複数の主体（エージェント）が互いに影響を及ぼし合うような状況において，個々の主体がどのような知識を獲得するのかを，一つの論理体系の中で簡潔に記述することが可能となった．

最近では，ゲーム理論をはじめとする種々のマルチエージェントシステムの分析に動的知識論理を応用する試みが，研究代表者らの研究を含め数多くなされている．しかしながら，この論理体系を暗号プロトコルの安全性検証に応用する研究は，Mardare や Dechesne らの研究などがあるものの，単純なプロトコルのみを対象としていることなどから，実際のプロトコルの安全性検証に適用するためには，多くの課題が残されていた．

２．研究の目的

本研究は，暗号プロトコルの安全性検証法を，動的知識論理をもとに構築することを目的に行われた．特に，プロトコルの実行によって参加者間で共有される知識の形成過程に注目し，その知識命題の成立の可否によってプロトコルの安全性を検証する方法の確立を目指した．以上のことを実現するために，本研究では以下の課題の達成を目標とした．

まず，プロトコルの実行過程と参加者の知識に関する推論を，動的知識論理をもとにした論理体系によって定式化する．その際，述語記号を導入せず，なるべく単純な体系で定式化することを目指した．

次に，この論理体系を用いて種々のプロトコルを分析することを通じ，知識命題の成立の可否と安全性との一般的な関係をもとにした検証法を構築する．ここでは特に，認証プロトコルや契約署名プロトコル，合理的秘密分散プロトコルなどを対象とする．

また，上記の検証法をもとに，論理体系における証明図の拡張や合成による安全性証明を行う方法についても検討することを目標とした．暗号プロトコルの設計では，コンポーネントとなる単純なプロトコルを拡張・合成することによって，より複雑なプロトコルを生成することがしばしば行われる．そこで，このプロトコルの生成過程にうまく対応させながら，コンポーネントの安全性に関する証明図を拡張・合成することによってプロトコルの安全性証明を行うというのが，この証明法のアイデアである．この手法は元来，PCL によって提案されたものであるが，PCL が動的論理をもとにした推論体系であることから，本研究の体系に対しても自然にこのアイデアが適用できるものと考えられる．

３．研究の方法

以上で述べた目的を達成するためのアプローチとして，まず動的知識論理をもとに，暗号プロトコルの安全性証明のための論理言語と公理系を与えることを目指した．先に述べたように，本研究の主要な関心は，参加者間で成り立つ知識命題がプロトコルの実行過程でどのように形成され，またその知識命題と安全性との間で成り立つ一般的な性質が何であるのかという問題である．こうした分析を見通し良く行い，かつ実用的な検証法を構築するために，ここで与える論理体系は極力単純なものにすることを目標とする．

動的知識論理における論理式は，一般に“$[\alpha_1;\alpha_2;\cdots;\alpha_n]\varphi$”という形をしており，

「$\alpha_1;\alpha_2;\cdots;\alpha_n$ が実行されるとφが成り立つ」ことを表す．本研究では，動的様相の“$[\alpha_1;\alpha_2;\cdots;\alpha_n]$”でメッセージの送受信などのプロトコルの実行過程を表し，また“φ”はこの実行後に成り立つ（知識様相を含む）命題を表す．既存研究では，この“φ”を構成する原子論理式に述語記号を導入し，またメッセージの送受信などの動作を表す命題を“φ”の中で顕在的に表現するものが多い．しかしながら，こうした言語を導入すると論理体系が複雑になってしまう．また本研究は，「プロトコルの実行過程で何が起こるのか」を証明するのではなく，「参加者間でどのような知識が共有されるのか」を証明することを目的とした．そのため，ここで扱う原子命題は，「参加者 A がプロトコルに従っている」や「参加者 A が（プロトコルの安全性に直接関わる認証子などの）情報 i を持っている」などの一般的な性質のみに絞り考察した．その上で，こうした原子命題について成り立つ知識命題の証明にのみ注目し，それ以外の概念はなるべく排除した論理体系の構築を目指す．なお，このような単純化を行っても，プロトコルの送受信や暗号化・復号化などの操作に関する推論は，動的様相の記述力だけで十分に定式化できると考えられる．さらに，この推論体系に対する意味論を，先に言及した Mardare や Dechesne らの研究などを参考にしながら与えることを目標とした．

次に，以上で得られた推論体系を用いて，様々な具体的なプロトコルの分析を行うことを目標とした．最初は Dolev-Yao モデルと呼ばれる攻撃者のモデルの範囲内での安全性のみを扱い，また比較的単純なプロトコルのみを対象とする．これにより，知識命題と安全性との間で一般的に成り立つ性質を，推論体系におけるメタ定理として示すことを計画した．ここでは特に，Strand Space モデルの研究で示された 3 種類のテストと呼ばれる性質のような，安全性の判定に有益な，いくつかの単純な性質の発見を目標としている．こうしたメタ定理を用いて，あるパターン化された命題（すなわち論理式“$[\alpha_1;\alpha_2;\cdots;\alpha_n]\varphi$”，ただしここで，“$\alpha_1;\alpha_2;\cdots;\alpha_n$”はプロトコルの実行列，“φ”は参加者間で共有される知識を表す論理式）を証明することによって，プロトコルの安全性を示す検証法の構築を目指した．

最後に，研究の進捗状況に応じて成果をさらに発展させる．具体的には，PCL のアイデアをもとにした証明図の拡張や合成による安全性検証法や，証明可能な知識命題による安全性概念の階層化，また安全でないプロトコルを改良する方法などについても検討することを計画した．

４．研究成果

前述の通り，本研究は，暗号プロトコルの安全性検証法を数理的技法（形式手法、または formal method）の一つである論理推論をもとに構築することを目的として遂行された．特に，知識論理と呼ばれる推論体系の一種である動的知識論理（Dynamic Epistemic Logic）を用いて，プロトコルの実行における参加者間での知識の形成過程を分析することにより，プロトコルの安全性を示す検証法の確立を目指して行われた．このような検証法においては，参加者間で成り立つ知識命題の形成過程に関する十分な記述力と，知識命題と安全性との間で成り立つ一般的な性質を分析できるだけの単純さが求められる．

このような目的のもとで研究を行った結果，まず命題論理をもとにした動的知識論理による定式化については，プロトコルの実行に関する諸性質を命題論理の範囲のみで記述することは難しいことが判明した．プロトコルの実行過程では，メッセージの表現が無限に存在することが主な原因である．

そこで，本研究では動的様相を排した一階述語論理による定式化を目指した．これによって得られた体型は，プロトコルの実行や安全性に関する性質を記述する能力は備えていたが，数多くの公理や推論規則を要するものであるため，実際に定理証明のような手法で検証を行うには，当初懸念されていた通り体系が複雑すぎるという課題が残された．

しかしながら，以上で得られた論理体系は，分散システムにおける合意形成などに使われるある種のプロトコルの検証法などへの応用の可能性を示唆するものであった．また，述語論理によるアプローチについては，体系が複雑になるという問題はあるものの，プロトコルの実行に関していくつかの仮定を置くことで，検証法として有用な体系に近づくことができたと考えられる．今後，これらの成果を取りまとめ，国際会議等で発表することを計画している．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 0 件）

〔学会発表〕（計 1 件）

① **Koji Hasebe**, Mitsuaki Tsuji, and Kazuhiko Kato. Deadlock Detection in the Scheduling of Last-Mile Transportation Using Model Checking. 査読有, *15th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2017)*, 8 pages, November 2017.

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
ホームページ等
http://www.cs.tsukuba.ac.jp/~hasebe

６．研究組織
(1)研究代表者
長谷部　浩二（HASEBE, Koji）
筑波大学・システム情報系・准教授
研究者番号：80470045