

論文審査の要旨及び担当者

No.1

報告番号	甲 乙 第	号	氏 名	阿部涼介
論文審査担当者	主 査	政策・メディア研究科委員	兼 環境情報学部教授	植原 啓介
	副 査	政策・メディア研究科委員	兼 環境情報学部教授	楠本 博之
		政策・メディア研究科委員	兼 環境情報学部教授	服部 隆志
		慶應義塾大学グローバルリサーチインスティテュート	特任教授	中村 修
		慶應義塾大学グローバルリサーチインスティテュート	特任教授	村井 純
		慶應義塾大学大学院 政策・メディア研究科	特任教授	鈴木 茂哉
学力確認担当者：				
阿部涼介君提出の学位請求論文は「情報システムにおける信頼に基づくクレームの妥当性検証」と題し、全9章から構成される。 人々は情報システムを活用し、情報をやり取りすることで、人々はその地理的關係にとられずグローバルな空間中で協調し、様々な活動が可能となった。その中で、やり取りされる情報の妥当性検証は一般性の高い営みであるにもかかわらず、そのモデルは確立されていなかった。また、関連して「信頼」の概念も盛んに議論されているものの、情報システム観点からその概念を捉え、情報の妥当性検証における意義を明確にしたモデルは存在しなかった。 本論文では、ある主張者が主張する情報である「クレーム」の妥当性検証に着目し、検証者自身の明示的な基準に基づき妥当性検証を担う情報システム構成する手法である Shinken モデルを「信頼」の概念の定義とともに提案している。本論文は、これまでデジタル証明書などの既存の議論において、その形式的な検証が主に議論されていたことに対して、より踏み込んで示される情報自体の妥当性を検証するモデルを確立し、情報システムとして実現可能であることを実証したことに新規性を有していると評価できる。 第1章では、人々が情報システムを通じて情報をやり取りしている中で、その情報の検証可能性が盛んに議論されている一方、情報の妥当性検証のモデルが十分に確立されていないことを指摘している。 第2章では、情報の妥当性検証をモデル化するため、関連する概念を整理し、そのやり取りのモデルを論述している。中でも、日本語の「検証」にあたる英語の概念として Verification (形式的な検証)と Validation (妥当性の検証)の違いを複数の標準文書に基づき整理し、本研究の基礎となるモデルを述べている。ここで、クレームの妥当性検証は検証者の「検証ポリシー」に示される検証基準にクレームが適合するか判定する営みであるとモデル化している。 第3章では、本論文に関連する要素技術を概説している。中でも、デジタル署名技術を活用するため、デジタル署名付きデータの抽象データモデルを整理し、その例として Verifiable Credentials などのデジタル証明書関連技術について整理している。 第4章では、第2章でモデル化された情報の妥当性検証を情報システムで処理するためのインターフェースとして抽象的な関数モデルを定義し、関数の実装として検証器を実				

装することで情報システムとしてクレーム検証を実現することであると論述している。また、既存の議論を参照しながらその課題を整理し、検証器に実装される検証基準は決定性があり、検証者の検証ポリシーの変更に追従し、改善できる更改可能性が必要であることを述べている。

第5章では、第4章で述べた特性を満たしながら情報システムで妥当性検証を実現するための **Shinken** モデルを提案している。**Shinken** モデルでは、検証ポリシーで示される検証基準に、計算機で決定困難な命題を含む可能性があることから、仮定を導入することで決定性と更改可能性のある基準を構成する。また、仮定を導入することで対象が真であることを期待することから、仮定を置くことをクレームの妥当性検証における「信頼」と整理している。

第6章では、具体的な事例において **Shinken** モデルに基づきクレームの検証基準を決定性のある形で構成するケーススタディを論じている。商取引の結果をクレームとした時、商取引の過程を記録する基盤としてブロックチェーン技術を適用し、その特性を信頼することで、検証基準を構成することを論述している。ブロックチェーン技術に基づくアプリケーションプラットフォームである **Ethereum** 上で商取引の過程を記録し、その結果を検証するシステムのプロトタイプを実装し、その実現可能性を実証している。

第7章では、**Shinken** モデルに基づき構成した検証基準が、更改可能であることをデジタル証明書の活用を対象に論述している。デジタル証明書の発行にあたり、証明書発行者である認定者が証明書に含まれるクレームの妥当性検証をする際に用いた根拠情報を証明書に紐づける手法を提案している。本手法により、検証基準を更改し、認定者が特定の根拠情報に基づき証明書を発行したことを検証可能であることをプロトタイプの実装とともに実証している。

第8章では、**Shinken** モデルに基づき第6章および第7章において、クレームを妥当性検証する情報システムを決定性と更改可能性のある形で構成できたことを分析している。また、それぞれにおいて共通する検証基準のモデルを抽出し、本論文で論じた事例以外にも応用可能性があることを述べている。また、**Shinken** モデルに基づき構成された検証基準はコンテキストに応じて様々なクレームに対して構成できることを述べ、本研究の提案が多様な対象に適用可能なことを論じている。

第9章では、本研究の総括をすると共に、今後の研究課題についても詳細な指摘が行われている。

阿部君は、2017 年よりブロックチェーン技術の活用を起点として、情報の検証可能性および信頼に関する研究に従事してきた。本博士論文は、それらの研究を踏まえて、情報の妥当性検証を実現する抽象的なモデルを確立しており、今後情報システムを活用したデジタル社会において、様々な情報の妥当性検証を実現する礎となる成果である。本成果は、阿部君がその専門領域であるデジタル署名およびその活用としてのデジタル証明書、ブロックチェーン技術など広範囲な技術に精通しつつ、抽象的なモデルを構成する阿部君の高い構成力によって実現されたものである。

論文審査の要旨及び担当者

No.3

本論文は、阿部君が研究者として、研究課題の発見および分析能力を有し、これら先端的な研究を行う為に必要な高度な研究能力、並びにその基礎となる豊かな学識を有することを示したものである。

よって学位審査委員会は、阿部君が博士（政策・メディア）の学位を受ける資格のあるものと認める。