

主 論 文 要 旨

No.1

報告番号	甲 乙 第	号	氏 名	阿部 涼介
主 論 文 題 目：				
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				
(内容の要旨)				
本研究は、主張者が主張するクレームの妥当性を検証者が判断する“クレームの妥当性検証”を情報システムで構成する抽象モデルを提案する。個人の実績証明や、多様化するシステムへのアクセスコントロール、フェイクニュースなどの偽情報に対して、デジタル証明書を活用した情報の妥当性検証が議論されている。デジタル証明書は様々な場面で繰り返し提示され、単体に限らず、複数の証明書を組み合わせて利用することも想定されている。しかし、証明書で示される情報であるクレームの妥当性検証は、既存のデジタル証明書の標準規格では検討の範囲外とされている。このため、典型的にはクレームの検証基準は特定のコンテキストに基づいて設計され、当該コンテキスト特有の仮定や条件が前提として組み込まれる。したがって、異なるコンテキストで特定のデジタル証明書を活用する場合、元々の前提を暗黙的に援用してしまい、目的に応じた適切な検証基準を構成できない恐れがある。そこで本研究では、デジタル証明書をはじめとする根拠情報を基に、検証者が自身のコンテキストに応じたクレームの妥当性検証を情報システムとして実現するモデルを提案する。まず、既存の証明書などを用いたやりとりをモデル化し、主張者が主張するクレームを、検証者が妥当とみなす検証基準を含む“検証ポリシー”への適合を判断する営みであると整理する。次に、検証ポリシーに基づき、情報システムで処理するための関数モデルを定義する。ここで、形式論理に基づいて情報システムでクレームを検証する際、検証基準には計算機で決定困難な命題を含むことがある。そこで、検証基準を構成する一連の命題の中で、特定の命題が常に真であると仮定することを“信頼”であると整理する。その上で、信頼し、真と仮定する命題を明示しながら決定論的な検証基準を構成する“Shinken モデル”を提案する。Shinken モデルに基づき、信頼する命題を明示することで、検証基準の透明性と更改可能性を担保し、検証者のコンテキストに応じたクレームの妥当性検証を実現する。本研究では、Shinken モデルに基づいたクレームの妥当性検証の実証として、2つのケーススタディを実施した。1つ目は、過去の商取引における結果を検証するために、ブロックチェーンを改竄困難な台帳であると信頼し、仮定した上で検証基準を構成する取り組みである。2つ目は、デジタル証明書を用いたクレームの妥当性検証において、証明書発行の根拠情報を証明書に紐付け、検証者が検証基準を更改する取り組みである。2つのケーススタディから、明示的な信頼に基づき検証基準を構成し、情報システムとしてクレームの妥当性検証を実現可能であると評価した。本研究の成果に基づき、				

コンテキストに応じて信頼する対象を明示しながら、複数の根拠情報を活用し、情報の妥当性検証を情報システムとして実現することが期待される。

キーワード: 1. クレーム検証, 2. 信頼, 3. 妥当性, 4. デジタル証明書, 5. デジタル署名