審 査 結 果 の 要 旨

論文題目「複数組織対応属性ベース暗号を用いた研究データ向けファイル共有システムに関する研究」

学位申請者　石橋　拓哉

本論文は、複数の組織が柔軟かつ安全に研究データを共有可能なファイル共有システムに関するものである。本論文で報告されている主な学術的成果は複数組織間で利用可能な属性ベース暗号（MA-ABE）を用いて実システム上で安全にファイル共有を可能にするための要件を整理し、それに対応する要素技術の選定、性能評価および具体的な処理手順の考案を行ったことである。

本論文の背景として、近年のクラウドコンピューティングの普及によりデータのバックアップやファイルの共有にオンラインストレージが利用される機会が増加してきており、データの安全性の確保が重要な課題であるという現状がある。これに対して、本論文は複数の組織で研究データが共有される場面において利便性や効率性を損ねることなく、安全にデータ共有をするシステムを実現することを目的としている。

本論文の構成は以下の通りである。

第 1 章は序論であり、本研究の背景の説明としてファイル共有システムの社会的要求と既存研究の事例とその問題点を明示し、さらに本研究の目的について明確に説明されている。序論として的確であり、学位申請者は当該分野において十分な知識を有していると判断できる。

第 2 章では、本研究に関連する既存研究と関連技術について詳細かつ的確に説明されている。さらに、それらの知見より複数組織間で利用可能なファイル共有システムの必要性を説明し、複数組織で利用可能なファイル共有システムで満たすべき要件について整理した上で明示されている。これらの学術的な価値は高いと判断され、申請者がこの分野に精通していることを示している。

第 3 章では、MA-ABE を用いた複数組織間で利用可能なファイル共有システムの構築方法について述べられている。まず初めに提案されている MA-ABE を網羅的に調査し、第 2 章で整理した要件を満たす MA-ABE を選定した。さらに、特に有望な候補として選定される Lewko の方式と Rouselakis らの方式を処理時間および公開パラメータサイズの比較を行い、現状で最も適している MA-ABE 方式が Rouselakis らの方式であることを明らかにした。次に、MA-ABE を用いた提案システムのユーザの鍵発行、データの閲覧、データの保存にかかる処理時間の計測・評価により、各処理が現実的な時間で動作することが示された。最後に、ユーザが人事異動や卒業時などに属性が変更された場合の鍵の失効方法に関して考察され、鍵の属性に有効期限を埋め込む方法が最適であることが示された。以上の検討により、複数組織で利用可能なファイル共有システムで満たすべき要件を満たすファイル共有システムの実現方法が明確化された。本研究以外で MA-ABE のような高機能暗号を実システムへ適用する事例は多くなく、本検討の学術的な価値は高いと判断される。

第 4 章では、第 3 章にて提案したファイル共有システムを実運用するための詳細な設計について述べられている。MA-ABE を用いた提案システムを社会で運用されているシステム等と連携して実現する場合、さらに満たすべき補助的な要件が新出することが示された。これらの補助的な要件を満たすために、提案システムにおける組織間での属性の取り扱いに関する方法、フ

ファイルの閲覧を制御するリストファイルの運用方法、ファイルの編集権限を制御するために必要となるアップロードマネージャの設置方法、鍵発行センターの運用方法に関して考察されている。次に、提案システムを実際に運用する際の処理手順に関する詳細設計が示され、その処理手順を実際のユースケースを想定して検証をしている。以上の結果、提案したファイル共有システムを実運用するための詳細な設計が明確化された。これらの内容は、理論的な検討のみではなく、現実のシステムとの連携も考慮したものとなっており、社会への波及効果も高いと判断された。

第 5 章では、本論文の結論が簡潔にまとめられており、本学位論文が高いレベルでまとめられていると判断された。

以上の結果、本論文は学位論文として十分な内容を有するものと審査委員全員の一致で判定された。

したがって、学位申請者　石橋　拓哉　氏は東海大学博士（工学）の学位を授与されるに値すると判断した。

論 文 審 査 委 員

主査	博士（工学）	高山　佳久	情報通信学部教授	（総合理工学研究科総合理工学専攻）
委員	博士（工学）	大東　俊博	情報通信学部教授	（総合理工学研究科総合理工学専攻）
委員	博士（情報科学）	村山　純一	情報通信学部教授	（総合理工学研究科総合理工学専攻）
委員	博士（工学）	山本　宙	情報通信学部教授	（総合理工学研究科総合理工学専攻）
委員	博士（工学）	森田　直樹	情報通信学部教授	（総合理工学研究科総合理工学専攻）
委員	博士（工学）	柿崎　淑郎	情報通信学部准教授	
委員	博士（工学）	金岡　晃	東邦大学理学部教授	