論 文 の 内 容 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

キーワード：ファイル共有システム，オンラインストレージ，複数組織間，
暗号文ポリシー属性ベース暗号，複数組織対応属性ベース暗号

近年，オンラインストレージサービスの普及により，個人でのデータのバックアップや，企業などのデータや会議資料等の管理にオンラインストレージが用いられることが増えており，オンラインでのファイル共有は DX には欠かせないものとなっている．オンラインストレージサービスではストレージの管理者により，アクセス制御やディスクごとに暗号化がされている．この処理はサービスの提供者側によって実施されているものであり，悪意のある管理者がいた場合，データを覗き見られる危険性がある．そのため，オンラインストレージを利用する際は，ユーザ側で暗号化を行い，データを保護するシステムが必要である．

利用者が自らデータを保護する方法として，公開鍵暗号の一種である，暗号文ポリシー属性ベース暗号（CP-ABE）を用いたファイル共有システムが既存研究で提案されている．CP-ABE は属性値(ID・所属・役職など）の論理式で表現されたアクセス権を暗号文に埋め込み，その暗号文のアクセス権を満たす属性を有したユーザの秘密鍵でのみ，復号可能にすることで，アクセス制御機能を暗号化処理に付加できる．ユーザは鍵発行センター(KGC）にて，自身の属性が含まれた秘密鍵を生成し，取得することで閲覧権限があるデータを復号できるようになる．CP-ABE を用いた既存のファイル共有システムでは，データの暗号化のみならず，ファイル名・ディレクトリ名の秘匿および編集権限の制御も行うことが可能な方式が提案されている．CP-ABE は単一の組織での使用を前提としているため，CP-ABE を用いた既存のシステムは単一組織での利用に限られる．ファイル共有システムを実際に利用する場面を考えた場合，共同研究等で研究データや論文の共有など，複数組織間でシステムを利用したい場面が想定される．しかし，既存研究の CP-ABE を用いたシステムでは，複数組織間のデータ共有には使用できず，これらのニーズに対応することができない．

本研究では，複数組織間で利用可能なファイル共有システムを実現することを目的と

し，具体的なシステムの構築方法を提案し，評価した．まず，複数組織間で利用可能なファイル共有システムが満たすべき要件を定義した．各要件を満たす方法として，複数組織対応属性ベース暗号（MA-ABE）を用いて，既存のファイル共有システムを複数組織間で利用可能にする方法を提案し，評価した．次に，MA-ABE を用いた提案システムを実運用する際に，システムの要件を満たす方法のより詳細な手法を提案・考察した．以上の提案・考察により，複数組織間で利用可能なファイル共有システムが実現可能であることを明確化した．

本論文は 5 章で構成されており，以下に各章の概要を示す．

第 1 章は序論である．本研究の背景と目的の説明として，ファイル共有システムの社会的要求と既存研究の概説をし，既存のファイル共有システムにおける課題を示し，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明らかにした．その後，本研究にて提案する，複数組織間で利用可能なファイル共有システムの実現方法を概説した．また，本論文の構成と各章の概要について述べた．

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説明した．まず，公開鍵暗号と CP-ABE について概説し，既存のファイル共有システムに用いられている暗号方式について説明した．次に，既存のファイル共有システムについて概説し，既存システムが複数組織間での利用ができないことを示した．その後，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を明らかにした．

第 3 章では，第 2 章で定義した要件を満たす，複数組織間で利用可能なファイル共有システムの提案した．初めに，提案システムに必要な要件を満たす方法として，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を提案した．次に，提案システムに用いる MA-ABE の方式を選定するため，先行研究にて提案されている MA-ABE の比較・評価を実施した．各方式の特性，公開パラメータのサイズの比較をした．さらに，アルゴリズムの実装・評価を行い，処理時間も比較した．その結果，Rouselakis らの方式が提案システムに最適であることを示した．その次に，Rouselakis らの方式の MA-ABE を用いたファイル共有システムにおけるユーザの鍵発行，データの閲覧，データの保存にかかる処理時間の計測・評価をし，各処理にかかる処理時間が現実的な時間で動作することを確認した．最後に，提案システムを運用する際に生じる問題点である，鍵の失効方法に関する提案・考察をした．その結果，鍵の属性に有効期限を埋め込む方法が現時点では最適であることを示した．以上の提案により，第 2 章にて定義した要件を満たす複数組織間で利用可能なファイル共有システムの実現方法を明確化した．

第 4 章では，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をした．MA-ABE を用いた提案システムを実運用する場合，第 2 章で明らかになった，複数組織間で利用可能なファイル共有システムが満たすべき要件を満たすために，さらに満たすべき要件が新出した．これらの要件を満たすため，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，KGC の運用方法に関する考察・設計をした．以上の考察によって，新出した要件を満たす詳細な提案システムの設計を示した．次に，提案システムを実運用する際に処理が発生する，ユーザの鍵発行，データのダウンロード・アップロードの詳細設計をした．また，詳細設計をした処理手順の実際のユースケースを想定した検証を行った．その結果，設計通りシステムを構築することで，提案システムが満たすべき要件を全て満たしていることを確認した．最後に，Rouselakis らの方式の MA-ABE 以外の方式を用いて，提案システムを構築する場合の提案システムの実現可能性の検討・考察をした．以上の提案・考察により，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に関して，実運用時の視点での運用課題の抽出やシステム構築方法の考察がされ，安全かつ実用的なファイル共有システムの実運用に関する方法が明確化された．

第 5 章は結論であり，本研究で得られた知見をまとめ，総括した．

以上のように本論文では，複数組織間で利用可能なファイル共有システムを実現する方法として，MA-ABE を用いて実現する方法を提案した．本研究の成果は，既存のファイル共有システムの問題点を解決し，ファイル共有システムに求められる複数組織間で利用可能である，ファイル共有システムの具体的な構築方法を示すことにより，今後のファイル共有システムの発展に貢献するものである．