東海大学紀要情報通信学部
Vol.16,2023,pp.11-20

論文

# 複数組織対応属性ベース暗号を用いたファイル共有システムの設計

石橋 拓哉[*1*2]，鈴木 智也[*3]，大東 俊博[*4]，土田 光[*6]，金岡 晃[*7]，柿崎 淑郎[*5]，相原 玲二[*8]

# Design of File Sharing Services using Multi-Authority Attribute-Based Encryption

by

Takuya ISHIBASHI[*1*2], Tomoya SUZUKI[*3], Toshihiro OHIGASHI[*4], Hikaru TSUCHIDA[*6], Akira KANAOKA[*7], Yoshio KAKIZAKI[*5] and Reiji AIBARA[*8]

( received on Apr. 28, 2023 & accepted on Jul. 18, 2023 )

**あらまし**

現在，属性ベース暗号（CP-ABE）を用いた様々なファイル共有システムが提案されている．従来のファイル共有システムの提案に使用されている CP-ABE は，単一組織での使用を前提としているため，これを利用したファイル共有システムは必然的に単一組織での使用が前提となってしまう．そこで本論文では複数組織で利用可能な属性ベース暗号（MA-ABE）を用いた，複数組織で利用可能なファイル共有システムの提案を行う．また提案するシステムを運用する際に生じると考えられる問題点に関しても考察を行う．

**Abstract**

Various file sharing systems using attribute-based encryption (CP-ABE) are currently proposed. The CP-ABE used in conventional file-sharing systems are based on the assumption that they can be used by a single organization. Therefore, a file sharing system based on CP-ABE is inevitably assumed to be used in a single organization. In this paper, we propose a multi-organizational file sharing system using Multi-Authority Attribute-Based Encryption (MA-ABE) that can be used by multiple organizations. We also discuss the problems that may arise when operating the proposed system.

**キーワード：**ファイル共有システム，暗号文ポリシー属性ベース暗号，複数組織対応
***Keywords:*** *File Sharing System, Ciphertext-Policy Attribute-Based Encryption, Multiple Authorities*

*1 総合理工学研究科総合理工学専攻 博士課程
Graduate School of Science and Technology, Course of Science and Technology, Doctor's Program
*2 情報技術センター 特定助手
Research and Information Center, Specified Research Assistant
*3 情報通信学研究科情報通信学専攻 修士課程
Graduate School of Information and Telecommunication Engineering, Course of Information and Telecommunication Engineering, Master's Program
*4 情報通信学研究科情報通信学専攻 教授
Graduate School of Information and Telecommunication Engineering, Course of Information and Telecommunication Engineering, Professor
*5 情報通信学研究科情報通信学専攻 准教授
Graduate School of Information and Telecommunication Engineering, Course of Information and Telecommunication Engineering, Associate Professor
*6 日本電気 特別研究員
NEC, Special Researcher
*7 東邦大学 教授
Toho University, Professor
*8 広島大学 上席特任学術研究員
Hiroshima University, Specially appointed senior research manager

## 1. はじめに

近年，柔軟なアクセス制御が可能な公開鍵暗号方式として暗号文ポリシー属性ベース暗号(Ciphertext-Policy Attribute-Based Encryption: CP-ABE)[1]が提案されている．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ポリシー（以下，アクセス権）を暗号文に埋め込み，その暗号文をアクセス権を満たす属性を有したユーザの秘密鍵でしか復号できなくすることで，きめ細やかなアクセス制御機能を暗号化処理に付加できる．CP-ABE ではユーザは鍵発行センター(Key GenerationCenter: KGC)に自身の属性が含まれた秘密鍵を発行してもらい，それを適切な認証を経て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．

閲覧権限に応じたデータの共有で代表的なアプリケーションにファイル共有がある．Google 社の Google ドライブやマイクロソフト社の OneDrive といったクラウドストレージに代表されるように，オンラインでのファイル共有は DX には欠かせないものであり，ファイル共有は ABE の最も期待される応用先と言って良い．CP-ABE を使ったファイル共有システムの先行研究として，CP-ABE を用いることでオンラインストレージ上のファイルの閲覧権限を柔軟に制御するシステム[2),3)]や，医療機関での電子カルテを担当医のみが閲覧可能なものから，緊急時に全スタッフが閲覧可能となるような変更を行える共有システム[4)]，従来のファイル共有サービスと異なり，コンテンツだけでなくファイル名/ディレクトリ名を含むディレクトリ構造全体を

暗号化し，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を行うシステム[5]などが提案されている．しかしながら，これらのシステムで使用している CP-ABE では，KGC は全てのユーザの秘密鍵を作成できる非常に強い権限を持っているため，利用組織内の信頼できる部署が管理することを想定しており，これにより単一の組織での使用を前提としている．そのため，CP-ABE を用いたファイル共有システムは複数組織間でデータを共有するなどの用途には向いていない．しかし実際これらシステムを利用することを想定した場合，例えば共同研究などを行っている場合では，研究データや論文などの共有を他組織のユーザと行いたいといった，複数組織間でのシステム利用をしたい場面が出てくることが考えられる．

複数組織で利用可能な属性ベース暗号(Multi-Authority Attribute-Based Encryption: MA-ABE) は複数の提案がされている[6), 7), 8), 9), 10), 11)]．著者らは MA-ABE を用いることにより複数組織間で利用可能とするファイル共有システムを実現するため，提案システムに用いるのに最適な MA-ABE の方式の選定や，属性管理，鍵失効時の処理の方法などについての考察など，実用的なユースケースを十分に考慮した様々な検討・提案を行ってきた[12)]．しかしながら，具体的なファイル共有システムとして実運用する際に必要となる，システムの処理手順や，様々なフォーマットなどに関しての設計は行っていない．そこで本論文では大東らのファイル共有システム[5)]の手法を参考に，文献[12)]で提案した複数組織で利用可能なファイル共有システムを実際に運用する際に必要となるシステムの処理手順やフォーマットに関しての設計を行う．実運用を考慮した際に生じると考えられる，提案するファイル共有システムにおける組織間での属性の取り扱いに関する問題点や，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や，KGC の運用方法に関する考察・設計なども行う．

本論文により，実運用を十分に考慮した複数組織間で利用可能なファイル共有システムの具体的な設計が提案されたことに加え，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．

## 2. 準備

本章では MA-ABE の説明で用いる対称ペアリング群について述べた後に，MA-ABE についての概説を行う．その後，大東らのファイル共有システムについて概説をする．

### 2.1 対称ペアリング群

対称ペアリング群 param = $(p, \mathbb{G}, \mathbb{G}_T, g, e)$ はそれぞれ，ビット長 $\lambda$ の素数 $p$，位数 $p$ の乗法的巡回群 $\mathbb{G}$, $\mathbb{G}_T$，生成元 $g \in \mathbb{G}$，多項式時間で計算可能な非退化性を有する双線形写像 $e: \mathbb{G}\times\mathbb{G} \rightarrow \mathbb{G}_T$ から成る．セキュリティパラメータ $\lambda$ を入力に取り，対称ペアリング群 param を出力するアルゴリズムを $\mathcal{G}_{\mathrm{SPG}}(1^\lambda)$ とする．

### 2.2 複数組織対応属性ベース暗号

属性ベース暗号[13)]の一種である CP-ABE[1), 14)]は，所属や役職などの属性を公開鍵として利用し，属性の論理式で表現されたアクセス権（例：人事部 OR（総務部 AND 部長））を暗号文に埋め込むことで復号可能なユーザを決定できる暗号方式である（Fig. 1）．ユーザは KGC に自分の属性（例: 人事，部長, ○○担当）が埋め込まれた秘密鍵を発行してもらい，秘密鍵に埋め込まれた属性集合が暗号文のアクセス権を満たすとき，暗号文を復号可能となる．しかしながら，CP-ABE の KGC は所属している全ユーザの秘密鍵を発行できる非常に強い権限を持つため，複数組織で共同利用を考えた場合には該当する KGC をすべての組織で信頼し共有しなければならず，KGC の分散管理は困難となる．そのため単一組織での利用が前提となってしまう．

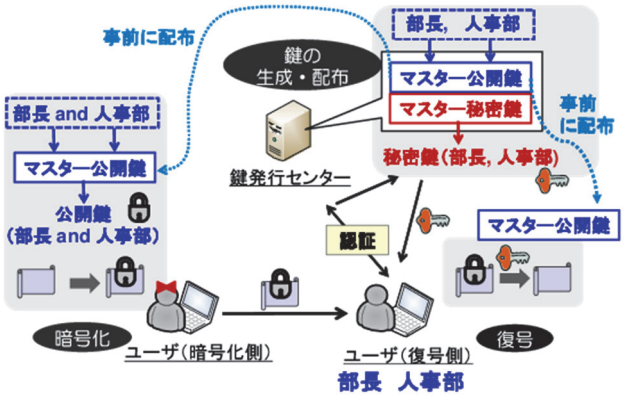


Fig. 1 Description of Ciphertext-Policy Attribute-Based Encryption

クラウドサービスなどの利用をする際には，複数の組織のユーザが共同で利用する場合が考えられる．こういった場合，単一組織のみでの使用が想定されている従来の CP-ABE では対応が不可能である，このような場面でも属性ベース暗号を複数組織で利用できるように，KGC を組織ごとに用意して複数組織で連携して使用できる方式である MA-ABE が提案されている（Fig. 2）．MA-ABE には大きく分けて，各組織の KGC を中央機関を使用して管理する方式[6)]と中央機関を必要とせず KGC が複数存在可能な方式[7), 8), 9), 10), 11)]が存在する．これらの方式は，複数組織で利用する場合などの現実的な属性管理ができるため，従来の KGC が 1 つのみの属性ベース暗号と比べ優れている．

中央機関を必要とせず複数の KGC が存在可能な属性ベース暗号では，ユーザ同士の結託攻撃に対する耐性を実現する必要がある．そこでこれらの方式では，MA-ABE を利用する全組織の全ユーザにおいて，ユーザごとに固有の識別子 GID を決め，KGC に依らず GID を秘密鍵生成の演算に含めることで結託耐性を与えている．たとえば，「A 大学教員かつ B 大学客員研究員」のユーザ向けの暗号文を解読するために「A 大学教員」と「B 大学客員研究員」がそれぞれ秘密鍵を提供し合ったとしても，それぞれの秘密鍵の GID が異なることから結合ができないため解読を防ぐことができる．

MA-ABE は様々な方式の提案がされているが，今回は Rouselakis 方式について説明をする．Rouselakis らの[7)]らの方式は以下の 5 つのアルゴリズムで構成される．

**Global Setup ($1^\lambda$):**

Global Setup はセキュリティパラメータ $\lambda$ を入力とし，グローバルパラメータ GP を出力する．GP には属性の母集団である $U$ や，KGC 番号である $\theta$ の母集団 $U_\Theta$ などが含まれる．

**Authority Setup (GP, $\theta$):**

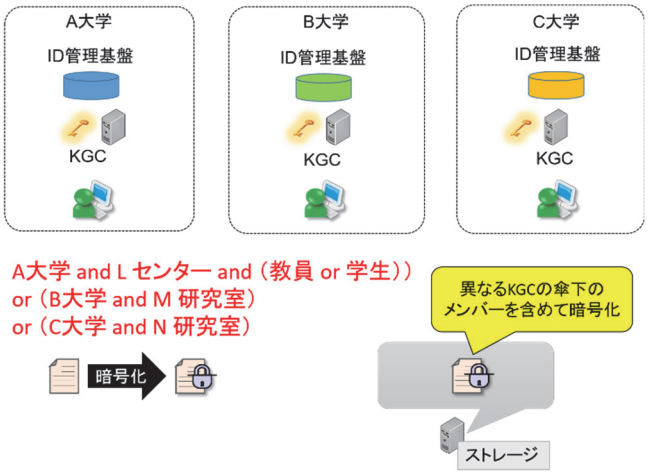


Fig. 2 Overview of the management of KGC in multiple organizations.

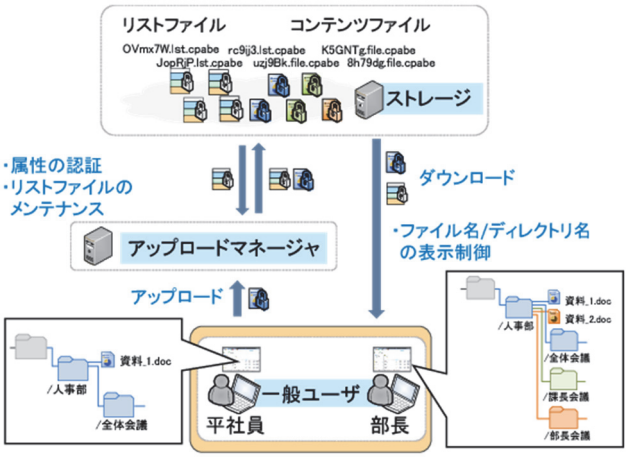


Fig. 3 Overview of Ohigashi et al.'s method[5]

Authority Setup は GP と KGC 番号 $\theta$ を入力とし，公開パラメータ $PK_\theta$ と秘密鍵 $SK_\theta$ を出力する．

**KeyGen (GID, $\theta$, $u$, $SK_\theta$, GP):**

KeyGen は GP，$KGC_\theta$ 内のユーザの属性情報 $u$，ユーザ固有の識別子である GID，$SK_\theta$ を入力とし，復号するユーザの秘密鍵 $SK_{GID,u}$ を出力する．

**Encrypt ($M$, ($A$, $\delta$), {$PK_\theta$}, GP):**

Encrypt は GP，データ $M$，アクセス構造 $A$，各属性に対応する公開鍵の集合 {$PK_\theta$} を入力とし，暗号文 CT を出力する．

**Decrypt (CT, {$SK_{GID,u}$},GP):**

Decrypt は GP，CT，{$SK_{GID,u}$} を入力とする．ここで，{$SK_{GID,u}$} に関連するユーザ GID の属性の集合 $\Gamma_{GID} := \{(GID, u)\}$ が CT に付与されたアクセス権を満たすなら，データ $M$ を出力する．そうでないならば，$\perp$ を出力する．

なお近年，Venemar と Alpar により MA-ABE に対する攻撃方法[15]が提案されている．しかし，この攻撃は中央機関を必要とするタイプの MA-ABE に対する汎用的な攻撃である．今回使用する Rouselakis らの方式[7]に対する攻撃は文献[15]の中で提案されておらず，また個別の攻撃方法も知られていない方式のため，現時点でこの方式は安全である．

### 2.3 大東らのシステムの概要

大東らによって CP-ABE を用いたファイル共有システムの提案[5]が行われている．大東らのファイル共有システムでは，CP-ABE を用いた従来のファイル共有サービスとなり，コンテンツだけでなくファイル名・ディレクトリ名を含むディレクトリ構造全体を暗号化し，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を行うシステムの提案をしている(Fig. 3)．これにより，ファイル名・ディレクトリ名からデータの内容に関する情報が漏れることを防いでいる．このシステムでは，ファイル名・ディレクトリ名はランダムな文字列に置き換えられ，その文字列と本来のファイル名・ディレクトリ名の対応をディレクトリごとのファイル(リストファイルと呼ぶ) で管理している．リストファイル内のファイル名・ディレクトリ名を閲覧が許可されているアクセス権ごとにまとめて CP-ABE による暗号化をすることで，高速に処理することを実現している．リストファイルは同じ属性を持つユーザが共有するため，同様の属性を持つユーザによってファイルの不正な書き換えや削除が起こることが考えられる．そこでこのシステムではディレクトリへのファイル・ディレクトリの追加処理を安全にするために閲覧権限と，編集権限を分けて制御を行う．これにはアップロードマネージャという登録専用のサーバを導入し，編集権限を集中管理する方法を用いている．アップロードマネージャでの処理も CP-ABE を用いた認証を利用することで，権限が無いユーザのファイルの登録も防いでいる．リストファイルとアップロードマネージャのフォーマットや処理手順などに関しては，3.3 節にて詳細な記述を行う．

## 3. MA-ABE を用いた複数組織で利用可能なファイル共有システムの提案

一般的に，従来のファイル共有システムは大学単位などの比較的大きな組織ごとに管理がなされている．しかしながら，実際のユースケースでは研究室単位や共同研究における研究グループごとなど，小規模な単位の組織間でデータにアクセスできるグループを作成したい場合がある．たとえば，複数の研究室間で共同研究を行っていた場合，大学単位で管理されている従来のファイル共有システムを使ったとすると，大学側の管理者に研究データを見られてしまう可能性がある．そのため研究グループ内にのみ公開したいデータを扱う場合には，このような使用方法は好ましくない．特に学外の研究機関と共同研究している場合，特に研究室単位で秘密保持契約 (Non-Disclosure Agreement:NDA) を締結しているような場合において，大学単位での KGC を持つシステムでは利用に適さない．データを共有したいユーザ間で秘密鍵を共有する方法も考えられるが，この場合データを共有したグループごとに異なる秘密鍵が必要となり，各ユーザが保有する鍵数が膨大になる可能性が高い．

著者らは従来のファイル共有システムにおける鍵管理の単位を，学部単位や研究室単位などの比較的小さな組織において管理を可能とすることを目的とした，複数組織で利用可能なファイル共有システムに最適な MA-ABE についての検討などを行っている[16),17),18)]．その結果，様々な MA-

ABE を多角的な視点から調査を行った結果, ファイル共有システムには Rouselakis らの方式を [7] 用いることが最適であることが分かった.

本章では, 従来研究にて提案を行ってきた複数組織間で利用可能なファイル共有システムを, 実利用可能なシステムとして提案を行う. その際, 提案システムを実際に運用するにあたって取り決めが必要となってくる, 問題点の解決策やシステムの運用方法についての考察・提案も行う.

### 3.1 提案システムの概要

本節では, MA-ABE(Rouselakis らの方式を [7])を用いて, 研究グループの責任者が秘密保持契約の代表者となるような場合にも対応し, 細分化した KGC の設置と管理を可能にした, 複数組織で利用可能なファイル共有システムの概説を行う. MA-ABE を用いることにより従来の CP-ABE を用いたファイル共有システムと異なり, KGC を複数設置することが可能となり, 秘密保持契約の代表者と KGC の管理者を一致させるような使用方法ができるようになる. これにより, 従来のファイル共有システムにおいて問題となる, 複数組織間での共同利用に関する問題の解決を行う. さらに提案システムでは大東らの従来のファイル共有システム [5] を参考に, ファイル名・ディレクトリ名を含むディレクトリ構造全体を暗号化し, ファイル名・ディレクトリ名および編集権限の制御も行う.

今回提案するシステムの設計を行うために, 以下の項目に関して特に詳細な設計を行う必要があると考えられる.

- 各組織における属性管理の方法
- リストファイルを用いたファイル名・ディレクトリ名の管理方法
- アップロードマネージャの運用方法と設置方法
- KGC の運用方法
- 属性変更時の鍵失効方法

MA-ABE を用いる際の属性管理は, 各組織間においてある程度の取り決めが必要となると考えられる. そのため属性管理の方法については 3.2 節にて考察・提案を行う. 今回参考にしている大東らの方式は単一組織で利用が想定されるファイル共有システムである. 提案システムは複数組織で利用可能なファイル共有システムであるため, リストファイルのフォーマットに関しては大東らの方式を参考に, 再構成を行う必要がある. そこでリストファイルのフォーマットに関して 3.3 節にて考察・提案を行う. またリストファイルの管理の際に必要となるアップロードマネージャの設置方法に関しても, 複数組織で利用可能な提案システムにおいて議論する必要がある. そこで提案システムにおけるアップロードマネージャの設置方法における考察・提案を 3.4 節にて行う. 提案システムでは MA-ABE を用いて複数組織で使用可能なファイル共有システムの実現を行っているが, MA-ABE において KGC がユーザの鍵を生成する際に使用する GID を, 提案システムを利用する全組織のユーザ全員がそれぞれ固有になるように管理する必要がある. そこで GID の管理を含めた KGC の管理に学術認証フェデレーション (学認) [+1] を用いる. 学認を用いた KGC の管理方法の詳細は 3.5 節にて説明する. 提案システムを運用するにあたって, ユーザの昇進や部署異動などによってユーザの属性が変更する場合が考えられる. そのような場合には, 変更前の属性の鍵を失効する必要が出てくる. そこでユーザの鍵失効に関する考察を 3.6 節にて行う.

+1 https://www.gakunin.jp/

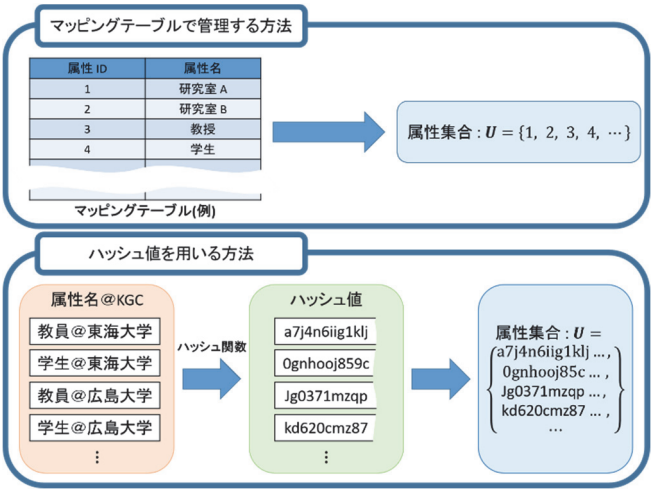


Fig. 4 Overview of attribute management methods

### 3.2 各組織における属性管理の方法

提案システムでは各組織における属性の管理方法の取り決めを行う必要がある, そこで本節ではその方法についての考察・提案を行う. 提案システムに用いる Rouselakis らの方式 [7] では, 安全性証明の要件を満たすため, 一度 Global Setup を行い属性集合 $U$ の領域を定義した後に, 新たに属性集合 $U$ に属性を追加することはできない. すなわちこれは提案システムの利用を一度始めた場合, 後から属性が増えた場合でもシステムの再セットアップをしない限り, 属性を追加することをできないことを意味している. しかしながら実際の利用シーンを想定した場合, 会社の部署や役職の新設や, 大学などの改組などにおける新しい属性の追加が必要となる場合が考えられる. そこで提案システムにおいて, システム利用開始後に新たな属性の追加が必要となった場合でも対応可能な, 属性の管理方法に関して考察を行う.

提案システムにおける上記の属性管理の問題に関しては, 事前にある程度の大きさの属性集合の領域を定義してシステムのセットアップを行うことにより, 対応することが可能と考えられる. しかし実際の利用シーンでは, システムの利用開始後に追加が必要となる属性の名前である, 新設される部署名や学部学科名, 研究室名などは新設されてからでないと分からないことが想定される. そのため事前に属性を用意して管理する場合に, 属性名の取り扱いが問題となる. そこで今回は 2 つの方法を考案し, 実際のシステムでの利用に適した方法についての考察・提案を行う.

#### 3.2.1 属性名をマッピングテーブルで管理する方法

属性名を番号などの ID で管理を行い, ID に対応する属性名をマッピングテーブル用いて管理を行う方法が考えられる. この方法ではまず最初の属性集合 $U$ の領域の大きさを決める際に, 属性を番号などの ID とみなして領域の確保を行う. その後, 確保した領域の属性の ID に実際に使用する属性の属性名を対応させる. 属性 ID と属性名の関係に関しては, Fig. 4 のような形で, マッピングテーブルを用いて管理を行う. この方法をとることにより, 提案システムを利用開始した後に属性を追加する必要が生じた場

合でも，使用していない属性 ID に新たな属性名を割り当てることにより対応することが可能となる．

この方法では属性を追加することが可能ではあるが，属性を追加する度にマッピングテーブルの更新を行う必要がある．さらに更新を行ったマッピングテーブルは，提案システムを利用する全組織で共有をする必要があるため，更新する毎に新しいマッピングテーブルを全組織に共有しなくてはならず，非常にコストがかかるといったデメリットが考えられる．

### 3.2.2 属性名にハッシュ値を用いる方法

属性名をハッシュ関数に入力し，出力されたそのハッシュ値を属性とみなして属性集合 $U$ で領域を確保する方法が考えられる．この方法ではまず KGC 番号と属性名を連結し（例：学生＠東海大学），この連結した属性名をハッシュ関数に入力し，出力されたハッシュ値を一つの属性とみなして属性集合 $U$ の要素の一つとして扱う．この時全ての KGC 番号において，提案システム上に存在する全ユーザの属性と連結をしてハッシュ値を取る．また KGC 番号は実際に使用する数よりも多く確保する必要がある．これにより，学部学科が増えたりした場合にも未使用の KGC 番号を割り当てることにより対応することが可能となる．そこで提案システムにはこの方法による属性管理が適用であると考える．

## 3.3 リストファイルを用いたファイル名・ディレクトリ名の管理方法

一般的なファイル暗号化システムではデータの暗号化のみを行うが，提案システムでは大東らのファイル共有システム [5] の手法であるリストファイルという概念を用いてデータの暗号化だけでなくファイル名・ディレクトリ名の暗号化および，編集権限の制御を行う（Fig. 3）．これにより，ファイル名などからデータの内容の情報が漏洩することを防止する．

今回参考にしている大東らの方式ではデータへのアクセス権のうち，データの又はファイル名/ディレクトリ名を復号できる権限を read 権とし，これらの作成や編集をすることのできる権限を write 権と定義している．そこで提案システムにおいても同様に定義を行う．提案システムでは read 権による制御は MA-ABE を用いて暗号化することで実現する．ファイルのデータ自体は MA-ABE で暗号化し，ファイル名はユニークな疑似乱数列で表される保存用ファイル名に置き換えて保存を行う．このとき，保存用ファイル名と元のファイル名の対応関係に関して MA-ABE で暗号化を行う．これにより read 権がないユーザからファイル名を秘匿することができる．write 権に関しては大東らの方式で提案されているリストファイルとアップロードマネージャーマネージャによって制御を行う（Fig. 3）．アップロードマネージャはリストファイル内の write 権に対応する属性をユーザが保有しているかを認証する．認証に成功した場合にのみ，アップロードマネージャはストレージへのファイルのアップロードおよびリストファイルの更新を行う．ユーザはこのアップロードマネージャを介してのみファイルのアップロードを行えるようにすることにより，権限のないユーザによる不正なデータの書き換えやファイル削除を防いでいる．ユーザはデータのダウンロードはストレージから直接行い，アップロードはアップロードマネージャを介して行う．この時のアップロードやダウンロードの処理に関しては，ファイルビューアを用いて行う．

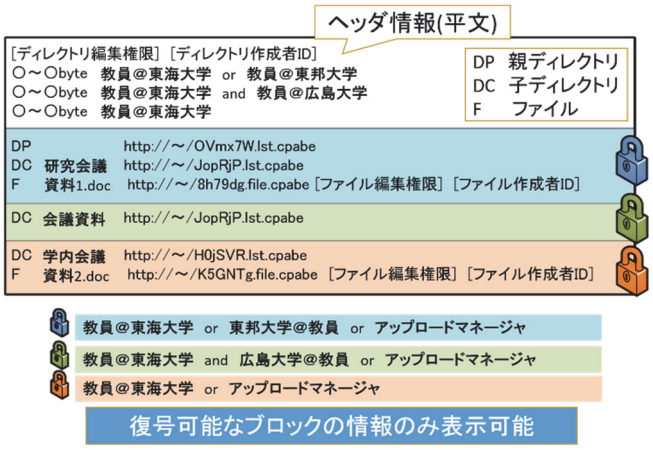


Fig. 5 Overview of list files

大東らのシステムでは単一組織での利用が想定されているが，提案システムは複数組織で利用することができる．そのため，リストファイルの大部分のフォーマットは大東らのシステムのものを使用するが，リストファイルのフォーマットを一部再考する必要がある．提案システムにおけるリストファイルでは，まずヘッダ情報の 1 行目は大東らのシステムと同様にカレントディレクトリの write 権を表す文字列およびディレクトリ作者の ID を記す（Fig. 5）．2 行目以降も同様にリストファイル内の read 権毎のブロックの開始位置をバイト数で表記を行い，その後ろにそのブロックの read 権を表す文字列を格納する．この時，提案システムは複数組織で使用可能であるため read 権に自組織以外のユーザの属性が入る場合がある．そういった場合には，自組織以外の属性が含まれている read 権のブロックを優先的にリストファイル上部から追加していく．そしてその下に自組織の属性のみのブロックを格納していく．こうすることにより，リストファイルを効率的に作成・復号することができる．

## 3.4 アップロードマネージャ運用方法と設置方法

提案システムではリストファイルを用いて，データの暗号化だけでなくファイル名・ディレクトリ名の暗号化および，編集権限の制御を行う．リストファイルを管理するには共有の属性などを作成し管理することができるが，この場合共有するユーザによって勝手にファイルの編集をされてしまう可能性がある．そこで大東らのシステムではアップロードマネージャを用いて集中管理する方法を用いている．アップロードマネージャでは，ファイルの編集権限のあるユーザによる要求が行われた場合にのみストレージへの書き込みを行なう．この際，編集権限の管理にはリストファイルを用いる．ファイルのダウンロードはストレージから直接行うことでアップロードマネージャの負荷の軽減を行っている．

アップロードマネージャの管理者はストレージの全ファイルの編集が行える権限を持つこととなる．そのため提案システムのような複数組織での使用を前提としているシステムでは，アップロードマネージャの設置場所および管理方法が問題となる．そこで本章ではアップロードマネージャの適切な設置場所・管理に関する考察を行う．

### 3.4.1 アップロードマネージャ運用方法と設置方法

大学や企業などの比較的大きな組織単位でアップロードマネージャを管理する場合について考える．前述の通り，アップロードマネージャは管理者が強い権限を持つこととなる．そのため，研究室などのさらに小さな組織単位で共同研究などを行っており，NDA などを結んでいた場合を想定するとこの管理方法は，研究室外の職員などが研究データ等の情報を取得できてしまう可能性がある．よってこの方法でのアップロードマネージャの管理は現実的ではない．しかしながら研究不正が発覚した際など，大学や企業などの監査を行うような一部の部署が研究データを見る必要がある場合が考えられる．このような場合に備え，研究グループのメンバー以外にこのような部署用の属性を作成しておき，全データのアクセス権に OR で追加するなどの工夫が必要になると思われる．

### 3.4.2 KGC を持つ組織毎の管理

提案システムの KGC を持つ組織毎にアップロードマネージャを管理する場合について考える．この場合 3.4.1 節で問題となった共同研究などを行っている場合でも，問題なくアップロードマネージャの管理が行えると考えられる．また KGC を持つ組織毎に管理を行うため，MA-ABE に置いて非常に強い権限を持つ KGC の管理者が既に存在すると考えられる．そのため，アップロードマネージャを管理するユーザの管理をこの管理者が行うことにより実現が容易となると思われる．提案システムでのアップロードマネージャの管理に関して，このように KGC を持つ組織ごとに管理する方法が有用であると思われる．またアップロードマネージャの運用には他組織のユーザの属性の公開パラメータも必要となる．そこでアップロードマネージャは一定の周期で，全組織の全ユーザの属性の公開パラメータを取得する必要がある．この時、毎回全ての公開パラメータを取得すると非常にコストが大きくなってしまう．そこで初回のみ全組織の全ユーザ分の公開パラメータを取得しアップロードマネージャに保存し，2 回目以降は必要に応じて定期的に新たに更新された差分の公開パラメータを取得し保存する方法を用いる．

### 3.5 KGC の運用方法

提案システムでは，暗号用の鍵の管理(KGC の管理) とユーザの ID 管理（GID の管理）を分けており，後者は各大学等で管理されている ID 管理基盤を利用することを想定している．しかしながら，各組織が独立に ID を管理する場合，GID を自由に付与することができ，2.2 節で述べた結託攻撃への防御が困難となる．したがって，異なる組織の ID 管理基盤が管理していても全ユーザで ID が異なるような GID の固有性を実現できる仕組みが必要となる．そこで,本システムでは上記の条件に合致したものとして，学術認証フェデレーション（学認）で用いている ePPN（eduPersonPrincipalName）を利用することを想定する (Fig. 6)．ePPN は「ユーザ ID@所属大学のドメイン名」のような形で構成されており，学認においてユーザを識別することのできる加盟組織内で固有の名前になっている．学認の仕組みを用いて提案システムを実現する場合，まず自組織の認証プロバイダ（IdP）で認証を行い認証情報（ePPN を含む）を発行する．その後，発行された認証情報を利用してユーザは鍵発行を依頼する組織の KGC（学認のサービスプロバイダ（SP）として構築する）で属性に対応する秘密鍵の発行を行う．このとき，認証情報に含まれる ePPN を利用することにより,ユーザ本人の GID に対応する属性の秘密鍵を発行することが可能となる．

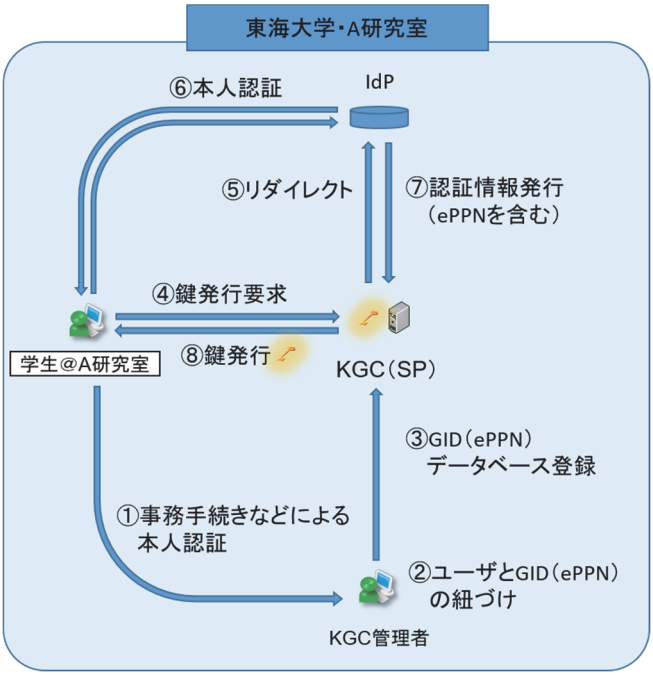


Fig. 6 Overview of key generation using GakuNin

KGC から発行される秘密鍵に対応する属性の管理については，3.2 節の方法にて行う．KGC を運営している組織では,所属しているユーザの各 GID に紐づける属性を事前にデータベース等に登録しておき，鍵生成の要求があったときに対応する秘密鍵を払い出すようにする．この登録については，当該組織で属性を持つ場合に何らかの事務手続きが生じると思われるため，その際に本人確認および対応付ける属性を精査した上で登録する．なお，ここで扱う属性の種類については，3.2 節の方法にて管理を行うため，学認などが提供しているような統一した属性を用いるなど，組織間で事前に取り決めを行う必要がある．その際，組織間で異なる属性を 1 つの属性で管理するなど，属性に範囲を持たせる場合が考えられる．この場合は属性がどの範囲までを包括するのか事前に詳細に取り決めを行い，範囲の誤解が生じないように注意する必要がある．

この方法では,上記のような GID と属性の紐づけなどの管理を研究室単位等で行わなければならないため，研究室教員等の KGC の管理者に一定の負担が生じることとなる．しかしながら，KGC の管理対象が研究室単位等まで小さくなったことから，比較的管理の負荷も小さくでき，MA-ABE を利用することによる安全性のメリットを考えた場合に許容範囲内となると考えられる．

### 3.6 属性変更時の鍵失効方法

提案システムに運用おいて，組織内でのユーザの昇進や部署異動，改組や卒業などによる属性変更などが起こることが考えられる．このような場合，属性変更前にユーザが所属していた部署のデータが，異動等をした後も全部署の鍵を保有していた場合，覗き見れてしまう可能性が問題となることが考えられる．このような事を防ぐため，著者ら

は過去にこのようなユーザの鍵失効方法に関しても議論している [12), 16)]．まず鍵失効機能を有する MA-ABE を用いる方法について検討を行った．しかしながら，当時提案されていた鍵失効機能付き MA-ABE は提案システムに使用するのに適していない方式しか提案されていなかった．そこで次に，代理人再暗号化を用いる方法について検討を行ったが，代理人サーバの運用コストが新たに生じてしまうため，適切ではないとの結論に至った．次に他のエンティティを用いた方法に関しても検討を行ったが，暗号化方式単体でのアクセス制御を実現するといった MA-ABE の利点を損なうため適切ではないとの結論に至った．その後，ユーザの鍵に有効期限を埋め込む方法に関して検討を行った．これはユーザの鍵の属性自体に「学生(2022 年度～2023 年度)」のようにあらかじめ有効期限を設定する方法である．この方法では鍵失効を柔軟に行うことができるため，提案システムにおいて最適であるとの結論に至ったため，提案システムの鍵失効方法にはこの方法を採用した．

文献 [12)] 発表時には，提案システムに適する鍵失効機能を有する MA-ABE が存在していなかったが，SecITC2022 にて提案システムに適していると考えられる Large Universe かつ鍵失効機能を備えた MA-ABE の提案がされている [19)]．これは方式自体が鍵失効機能を有しており，ユーザの鍵に有効期限などを埋め込むなどの工夫をすることなく，必要なタイミングで MA-ABE の方式自体の機能によって鍵失効を行うことができる方式となっている．そのため，今回の提案システムの実装・評価を行う際はこの MA-ABE の方式を用いて行うことが有益である可能性があるが，この方式を用いた実装・評価を含めた検討は今後の課題とする．

## 4. 提案システムの処理手順

本章では提案システムを実際に運用する際の，処理手順を示す．処理手順に関してはユーザの鍵発行時の手順と，データのダウンロード時とアップロード時の手順に分けそれぞれ説明を行う．

### 4.1 鍵発行時の処理手順

Fig. 7 にユーザの鍵発行時の処理手順を示す．鍵発行を行う KGC に関しては 3.5 節にて説明をおこなったように，学認の仕組みを用いて SP として管理を行う．以下に鍵発行時の処理手順の説明を示す．

**（K-1）本人認証**
KGC 管理者はユーザに対して，事務手続きなどによる本人確認を行う．

**（K-2）ePPN と認証ユーザ紐づけ**
KGC 管理者は本人認証を行ったユーザとそのユーザの ePPN の紐づけを行う．

**（K-3）ePPN と対応属性のデータベース登録**
KGC 管理者はユーザと紐づけを行った ePPN に対して，その ePPN がどの属性を有するかを判断し，その ePPN に対応する属性を KGC のデータベースに登録する．

**（K-4）鍵発行要求**
ユーザは自組織の KGC に対して，自身の秘密鍵を取得するため鍵発行要求を行う．

**（K-5）リダイレクト**

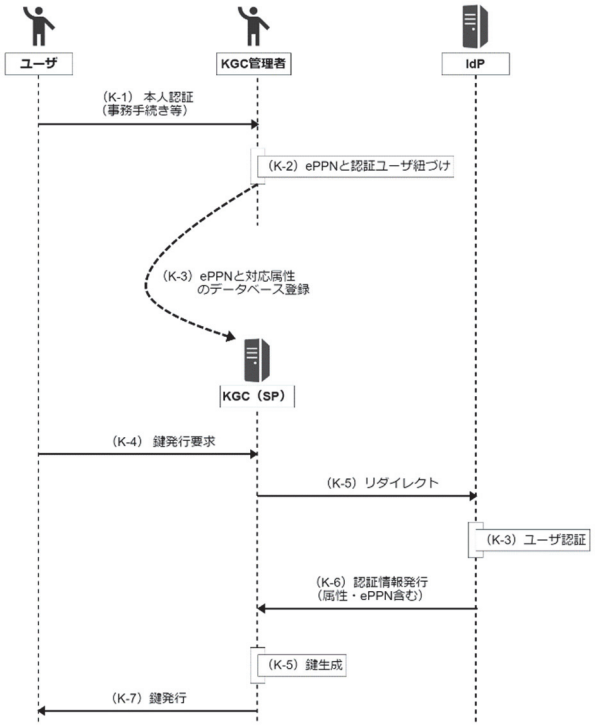


Fig. 7 Processing for key generation

KGC はユーザの鍵発行要求を受けたユーザの認証を行うため，認証プロバイダである IdP にリダイレクトを行う．

**（K-6）ユーザ認証**
ユーザは IdP の認証画面にて認証を行う．

**（K-7）認証情報発行**
IdP は認証完了後，認証を行ったユーザの認証情報を発行する．この時の認証情報には ePPN が含まれる．

**（K-8）鍵発行鍵**
KGC は IdP によって発行された認証情報をもとに，ユーザの秘密鍵を生成する．その後，生成を行った秘密鍵をユーザへ発行する．

このときユーザは他組織においても属性を保有している場合は，別途同様の手順を所属している全組織において行う．

### 4.2 ダウンロード時の処理手順

Fig. 8 にデータのダウンロード時の処理手順を示し，以下
にその説明を示す．

**（D-1）ディレクトリ選択**
ユーザはデータをダウンロードするストレージのディレクトリ名をビューア上で確認し，移動先ディレクトリを選択する．

**（D-2）リストファイル取得**
選択したディレクトリのリストファイルをストレージから取得する

**（D-3）リストファイル復号**
取得したリストファイルをユーザの秘密鍵にて復号する．

**（D-4）ファイル名・ディレクトリ名表示**
リストファイル復号後，「ファイル名・ディレクトリ名」

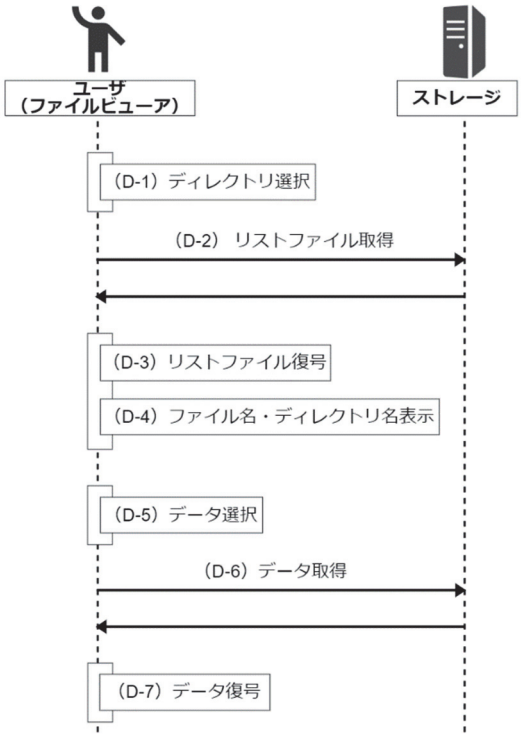


Fig. 8 Processing for download of data from storage

「そのファイル・ディレクトリの read 権・write 権」「ファイル名・ディレクトリ名」を表示する．

**（D-5）データ選択**

ビューアに表示されているファイル名を選択する．

**（D-6）データ取得**

選択したデータをストレージから取得する．

**（D-7）データ復号**

取得したデータをユーザの秘密鍵で復号する

リストファイルは大東らのシステムを参考にしているため，ルートリストファイルを起点として，ディレクトリ構造を相対パスで保持するようになっており，（D-1）～（D-4）によるディレクトリの移動を繰り返すことにより目的のデータがあるディレクトリに到達する．

### 4.3 アップロード時の処理手順

Fig. 9 にデータのアップロード時の処理手順を示し，以下にその説明を示す．

**（U-1）ディレクトリの移動**

ダウンロード時と同様，この手順をファイルをアップロードするディレクトリに到達するまで繰り返す．

**（U-2）ビューア操作**

次にユーザはビューア上にて「ファイルのアップロード」を選択し，「アップロードするファイルの選択」および「データの read 権・write 権の選択」を行う．選択操作完了後アップロードマネージャに「ファイルのアップロード要求」が通知される．

**（U-3）ユーザ認証**

アップロードマネージャはチャレンジをユーザに送信し，ユーザはそれに対して write 権に対応する秘密鍵で署名を行い，その署名文を返す．これにより，ユーザが write 権を満たす属性を有しているかを確認する．同時に「操作を行うディレクトリのリストファイルの URI」および（U-2）で決定した「データの read 権・write 権」「ファイル名の平文」を送信する．

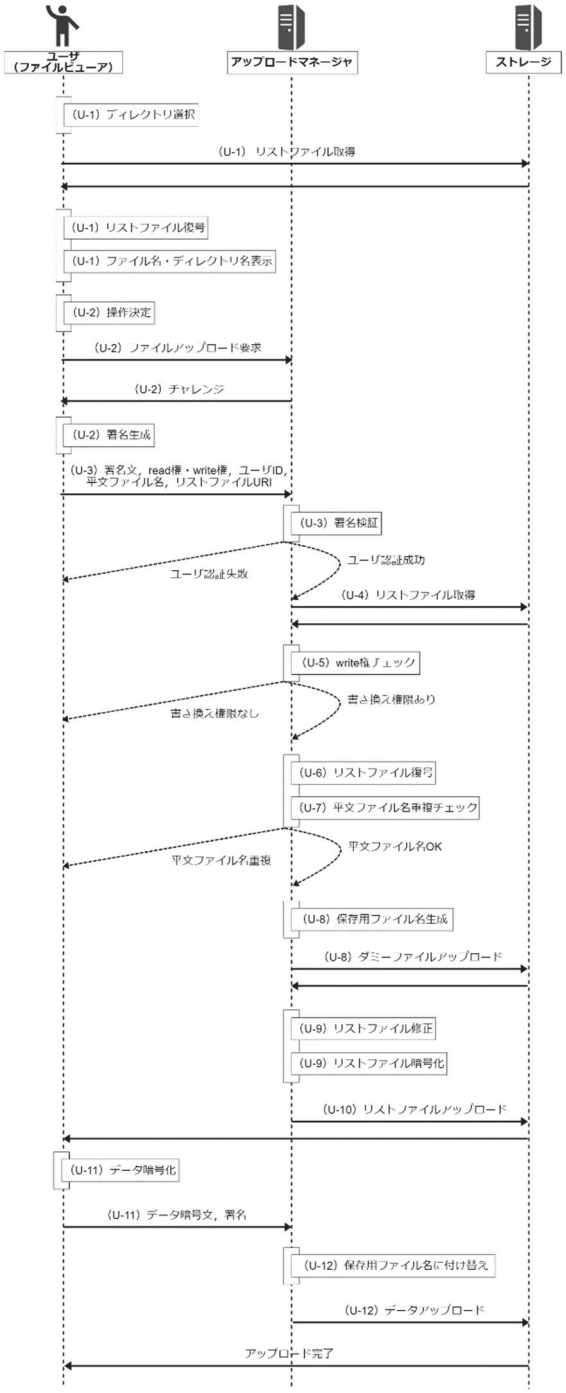


Fig. 9 Processing for uploading data to storage

**（U-4）リストファイル取得**

ストレージからリストファイルを取得し，リストファイルをロックする．

**（U-5）write 権チェック**
リストファイルのヘッダを参照し，ユーザが提示した write 権で書き込むことが可能か否かをチェックする．

**（U-6）リストファイル複合**
ヘッダを参照し，ユーザの read 権と一致するブロックの複号を行う．

**（U-7）平文ファイル名重複チェック**
復号したブロックの中に重複するファイル名がないかチェックする．

**（U-8）保存用ファイル名生成**
保存用ファイル名として疑似乱数を生成する．保存用ファイル名がストレージ上に存在しないことを確認した上で，予約処理としてサイズが小さいダミーファイルに保存用ファイル名を付けてアップロードしておく．もし既にストレージ上にファイルが存在していれば，保存用ファイル名の生成からやり直す．

**（U-9）リストファイル修正**
アップロードするファイルに関する行をブロックに追記してブロックを暗号化する．ブロックサイズ変更に伴うヘッダ情報の修正を行う

**（U-10）リストファイルアップロード**
リストファイルをストレージにアップロードする．アップロード完了後にリストファイルのロックを解除する．

**（U-11）データ暗号化**
ビューアでデータの暗号化を行う．

**（U-12）データアップロード**
アップロードマネージャは暗号化したデータを保存用ファイル名に付け替え，ストレージにアップロードしてダミーファイルを上書きする．

（U-9）のリストファイル修正時に暗号化ブロックを追加する場合，その属性の公開鍵が必要となる．そのため，アップロードマネージャは全組織の全属性の公開鍵を一定の周期で取得を行い，あらかじめ保存しておく．この時、毎回全ての公開鍵を取得すると非常にコストが大きくなってしまうため，システム立ち上げ時のみ全組織の全属性分の公開鍵を取得しアップロードマネージャに保存する．2 回目以降は必要に応じて新たに更新された差分の公開鍵を取得し保存する．

## 5. まとめ

本論文では複数組織対応属性ベース暗号（MA-ABE）を用いたファイル共有システムに関して，具体的な運用方法や運用時に問題となる点を考慮した上での設計・提案を行った．まず初めに複数組織間で利用可能なファイル共有システムの概要の提案を行った．その結果，提案システムを実際に運用する際には「各組織における属性管理の方法」，「リストファイルを用いたファイル名・ディレクトリ名の管理方法」，「アップロードマネージャの運用方法と設置方法」，「KGC の運用方法」，「属性変更時の鍵失効方法」について詳細に設計する必要があることが分かった．以上の点に関して検討を行った結果，各組織における属性管理方法には属性名にハッシュ値を用いる方法が最適であり，リストファイルを用いたファイル名・ディレクトリ名の管理に関しては大東らの方式 [5] の手法を参考に用いる方法が最適であることが分かった．またアップロードマネージャの運用方法と設置方法に関しては，KGC を持つ組織ごとに管理を行う方法が最適であり，KGC の運用方法は学認で用いられる ePPN を利用する方法が実現可能であることが分かった．さらに属性変更時の鍵失効方法に関しては，著者らが過去に検討を行った [12), 16)]，鍵の属性に有効期限を埋め込む方法を用いることにより，実現可能であるとの結論に至った．最後に，以上の点を考慮した提案システムの詳細な処理手順の設計を行った．

以上のように，本論文では MA-ABE を用いたファイル共有システムの実現を目指し，実際の運用時に必要となると考えられる問題点などを考慮し，それに対応する設計を行った．今後の課題として，本論文の提案ファイル共有システムを実際のストレージなどと組み合わせて実装行い，評価を行うことがあげられる．

**謝辞**　本研究の一部は JSPS 科研費（課題番号 JP16H02808, JP20K11811, JP22K12034）の助成, JST, CREST, JPMJCR22M4 の支援を受けたものである．

## 参考文献

1) Bethencourt, J., Sahai, A. and Waters, B.: Ciphertext-Policy Attribute-Based Encryption, 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA, pp. 321–334 (2007).
2) Zhao, F., Nishide, T. and Sakurai, K.: Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems, Information Security Practice and Experience - 7th International Conference, ISPEC 2011, Guangzhou, China, May 30 - June 1, 2011. Proceedings, pp. 83–97 (2011).
3) 松本悦宜，苦木大輔，内田恵，近藤伸明，満永拓邦，五十嵐寛，力宗幸男： 属性ベース暗号を用いたオンラインストレージサービス用クライアントの実装評価，信学技報， Vol. 111, No. 382, pp. 73–78 (2012).
4) 竹尾淳，稲吉陽一朗，白石善明，加藤昇平，矢口隆明，岩田彰ほか： HPKI 認証の特長を考慮した在宅医療介護システムにおける患者情報の開示先制御，情報処理学会論文誌，Vol. 60, No. 6, pp. 1228–1237 (2019).
5) 大東俊博，後藤めぐ美，西村浩二，相原玲二： 暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価，情報処理学会論文誌，Vol. 55, No. 3, pp. 1126–1139 (2014).
6) Chase, M.: Multi-authority Attribute Based Encryption,Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands,February 21-24, 2007, Proceedings, pp. 515–534 (2007).
7) Rouselakis, Y. and Waters, B.: Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption, Financial Cryptography and Data Security- 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers, pp. 315–332 (online), DOI: 10.1007/978-3-662-47854-7 19 (2015).
8) Lewko, A. B.: Functional encryption: new proof techniques and advancing capabilities, PhD Thesis (2012).
9) Lewko, A. and Waters, B.: Decentralizing attributebased encryption, Annual International Conference on the Theory and Applications of Cryptographic Techniques,Springer, pp. 568–588 (2011).
10) Okamoto, T. and Takashima, K.: Decentralized Attribute-Based Signatures, Public-Key Cryptography - PKC 2013 - 16th

International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings, pp. 125–142 (2013).

11) Datta, P., Komargodski, I. and Waters, B.: Decentralized Multi-authority ABE for DNFs from LWE, Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I (Canteaut, A. and Standaert, F., eds.), Lecture Notes in ComputerScience, Vol. 12696, Springer, pp. 177–209 (online), DOI: 10.1007/978-3-030-77870-5 7 (2021).

12) 石橋拓哉，小林海，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二： 複数組織対応属性ベース暗号を用いたファイル共有システムの実現可能性に関する考察, 情報処理学会論文誌， Vol. 64, No. 3, pp. 670–686（オンライン）, DOI: 10.20729/00225261 (2023).

13) Sahai, A. and Waters, B.: Fuzzy Identity-Based Encryption, Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, pp. 457–473(2005).

14) Waters, B.: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization, Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings (Catalano, D., Fazio, N., Gennaro,R. and Nicolosi, A., eds.), Lecture Notes in Computer Science, Vol. 6571, Springer, pp. 53–70 (online), DOI: 10.1007/978-3-642-19379-8 4 (2011).

15) Venema, M. and Alp´ar, G.: A Bunch of Broken Schemes: A Simple yet Powerful Linear Approach to Analyzing Security of Attribute-Based Encryption, Topics in Cryptology - CT-RSA 2021 - Cryptographers' Track at the RSA Conference 2021, Virtual Event, May 17-20, 2021, Proceedings (Paterson, K. G., ed.), Lecture Notes in Computer Science, Vol. 12704, Springer, pp. 100–125 (online), DOI: 10.1007/978-3-030-75539-3 5 (2021).

16) 石橋拓哉，小林海，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二： 複数組織対応属性ベース暗号を用いたファイル共有システムの評価および考察, 研究報告インターネットと運用技術(IOT)， Vol. 2019, No. 30, pp.1–8 (2019).

17) 石橋拓哉，鈴木達也，伊藤勝彦，大東俊博，相原玲二：属性ベース暗号を用いたファイル共有サービスの複数組織対応に関する考察，電子情報通信学会技術研究報告=IEICE technical report: 信学技報， Vol. 117, No. 472, pp. 79–84 (2018).

18) 石橋拓哉，大東俊博，土田光，金岡晃，柿崎淑郎，相原玲二ほか： 複数組織対応属性ベース暗号を用いたファイル共有システム，インターネットと運用技術シンポジウム論文集，Vol. 2018, pp. 16–23 (2018).

19) Ishibashi, T., Ohigashi, T. and Tsuchida, H.: Unbounded Revocable Decentralized Multi-Authority Attribute-Based Encryption Supporting Non-monotone Access Structures, Innovative Security Solutions for Information Technology and Communications - 15th International Conference, SecITC 2022, Virtual Event,December 8-9, 2022, Revised Selected Papers (Bella, G.,Doinea, M. and Janicke, H., eds.), Lecture Notes in Computer Science, Vol. 13809, Springer, pp. 320–339 (online),DOI: 10.1007/978-3-031-32636-3 19 (2022).