秘密分散法と属性ベース暗号を組み合わせたアクセス制御可能なデータ管理システム

奥 雅和[1,a)]　猪俣 敦夫[2,3]　新井 イスマイル[2]　藤川 和利[2]

概要：コストやアクセスのしやすさを理由にクラウドストレージを活用してデータを保存・共有するユーザが増加しているが，第三者によるデータの漏えい等の機密性の問題が存在する．秘密分散法を用いることで，そのような問題を改善する研究が行われている．しかし秘密分散法を用いることで，クラウドストレージを複数のユーザで共有するためのアクセス制御の設定に手間がかかり，利便性が低下するという問題が発生する．そこで本研究では，秘密分散法と属性ベース暗号を用いるシステムを提案する．そのシステムは秘密分散法によりクラウドストレージの機密性の問題を解決するとともに，属性ベース暗号により各ユーザのアクセス制御の管理コストを軽減する．

キーワード：クラウドコンピューティング，公開鍵暗号，アクセス制御

An access controling data management system using the combination of secret sharing scheme and attribute-based encryption

Masakazu Oku[1,a)]　Atsuo Inomata[2,3]　Ismail Arai[2]　Kazutoshi Fujikawa[2]

Abstract: The number of users sharing data with cloud storage is increasing under favor of low cost and accessibility. However, have a problem of confidence such as an outsider leaks data. There are researches improving such problem by using secret sharing scheme. However users' labor of access control for sharing among cloud storages still remains. This paper proposes the system using secret sharing scheme and attribute-based encryption. The system solves the problem of confidence and classifies data which users can access by using secret sharing scheme and attribute-based encryption.

Keywords: cloud computing, public key encryption, access control

1. はじめに

初期投資のコストの安さやインターネットに接続していればどこからでもアクセス可能であることを理由に，クラウドストレージサービスを利用する企業やユーザが増加している．ユーザ間でのデータのやり取りや共有をクラウドサービスを利用して行うユーザも多い．しかし，クラウドストレージサービスには機密性に問題があり，クラウドストレージに保存されているデータの漏えい等が発生する可能性がある [1], [2], [3]．これはクラウドストレージの管理や運用がクラウドサービスプロバイダによって行われ，不特定多数のユーザによるアクセスがあるからである．このようなクラウドサービスの問題の改善を目的とした研究も行われている．

クラウドストレージの機密性を向上させる方法として，秘密分散法 [4] を用いる研究が行われている．秘密分散法では秘密にしたいデータから複数の分散データを生成し，

1 奈良先端科学技術大学院大学情報科学研究科
Graduate school of information science, Nara institute of science and technology
2 奈良先端科学技術大学院大学総合情報基盤センター
Information initiative center, Nara institute of science and technology
3 東京電機大学
Tokyo denki university
a) oku.masakazu.ob8@is.naist.jp

生成された分散データのうち分散時に決めておいた閾値以上を集めることで元のデータを復元できる．閾値未満の分散データからは元のデータを復元することはできない．このことから，クラウドストレージに保存されている分散データの一部が漏えいしたとしても閾値以上の分散データが集まらなければ，元のデータを復元することはできず，元のデータの漏えいを防ぐことができる．秘密分散法を用いたデータ管理システムとして，分散データを複数のクラウドストレージで管理する方法が考えられる．この方法ではデータの共有を行うために各クラウドストレージのアクセス制御機能を用いて，分散データにアクセスするユーザのアクセス制御を行う必要がある．しかし，このアクセス制御の設定を各クラウドストレージに行うことは，システムを使用するうえで大きな負担になり，システムの利便性を損なうことになる．また，複数のクラウドストレージサービスプロバイダが協力した場合，分散データのうち閾値以上を集める可能性があり，元のデータが復元されてしまうという問題も存在する．

そこで，そのような問題を解決する方法として属性ベース暗号 [5] が考えられる．属性ベース暗号では，復号条件と属性情報を利用して暗号化と復号処理を行う．この復号条件を満たす属性情報を持つユーザは，復号処理が可能である．このことから，復号条件によって柔軟にアクセス可能なユーザを設定することが可能である．属性ベース暗号のこの特徴を用いることによって，前述の秘密分散法を用いたデータ管理システムの問題点を解決する．

本稿では，秘密分散法と属性ベース暗号を組み合わせた暗号化・復号処理を行うシステムの提案と実装を行う．提案システムは秘密分散法によりクラウドストレージサービスの機密性の問題を解決する．また，秘密分散法を用いたクラウドストレージではグループでのデータ共有が困難になってしまう問題とクラウドストレージサービスプロバイダの共謀によるデータの漏えいの問題を属性ベース暗号を用いることで解決する．

2. 関連研究

秘密分散法を用いたクラウドストレージのデータ管理システムを提案している先行研究が行われている [6]．先行研究では，秘密分散法と鍵を用いた暗号化処理を行い，暗号化データを複数のクラウドストレージで管理するシステムを提案している．その手法によってクラウドストレージの機密性の問題を解決している．また，属性ベース暗号を用いたクラウドストレージでのデータ管理に関する研究も行われている [7]．多数のユーザがデータを共有するクラウドストレージサービスでは，鍵管理の負担が大きくなるため既存の公開鍵暗号方式は適していない．先行研究では，この問題を解決するために，属性を指定して暗号化を行う属性ベース暗号を提案し，実装と評価を行っている．

秘密分散法のみのシステムでは，悪意のあるユーザが秘密分散法で生成した分散データのうちの閾値以上のデータを集めることが可能な場合，元のデータを手に入れることが可能である．ただし，分散データのうちの閾値未満のデータが紛失したとしても，元のデータを復元可能なことから冗長性が高いといえる．属性ベース暗号では，共謀・盗聴による元のデータの漏えいを防ぐことが可能で，復号条件と属性情報を用いることでユーザに応じて細かくアクセス制御を行うことができる．ただし，暗号化されたデータが紛失した場合，元のデータの復元は困難である．

3. 秘密分散法

秘密分散法の代表例として，Shamir の (k, n) 閾値秘密分散法がある．Shamir の (k, n) 閾値秘密分散法は，元のデータから分散数 n 個のデータを生成する．分散数 n 個のデータのうち，閾値 k 個以上を集めることで秘密情報を復元できる．閾値 k 個未満の分散情報からは，秘密情報についての一切知ることはできない．ただし，閾値 k 個以上のデータを取得していれば誰でも元のデータを復元可能で，復元を実行するユーザが正規のユーザかどうか判断できないという特徴を持つ．

4. 属性ベース暗号

一般的な公開鍵暗号方式では，暗号化で用いる公開鍵 PK と復号で用いる秘密鍵 SK は一対一の関係である．それに対して属性ベース暗号はマスター秘密鍵 SK と，マスター公開鍵 PK を用いて生成された暗号文 ct_Υ:=Encrypt(PK, M, Υ) の間のアクセス制御をすることが可能である．生成された暗号文 ct_Υ は $R(\Psi, \Upsilon) = True$ となるような関係 R が成り立つ場合のみ，ユーザ秘密鍵 SK_Ψ で復号可能である．このとき，パラメータ (Ψ, Υ) はそれぞれ復号鍵，暗号文に関連したパラメータである．

属性ベース暗号の代表例として，暗号文規定型属性ベース暗号（CP-ABE）[8], [9] と鍵規定型属性ベース暗号（KP-ABE）[10] がある．

CP-ABE の概要を**図 1** に示す．CP-ABE では，パラメータ Υ は属性情報と閾値ゲートを用いたアクセス構造であり，パラメータ Ψ は復号鍵を持つユーザの属性情報を表している．CP-ABE では，属性情報 Υ がアクセス構造 Ψ を満たす場合のみ，関係 $R(\Psi, \Upsilon) = True$ が成立する．したがって，一つのマスター公開鍵 PK でアクセス制御を細かく設定することができる．このような CP-ABE の特徴が，本稿で提案するシステムの属性ベース暗号に適しているため，提案システムでは CP-ABE を用いる．

CP-ABE は Setup，Key Generation，Encrypt，Decrypt の 4 つのアルゴリズムから構成される．

- Setup($1^\lambda, \vec{n} := (d; n_1, ..., n_d)$):
  1^λ(λ：セキュリティパラメータ)，最大属性数 d，属性

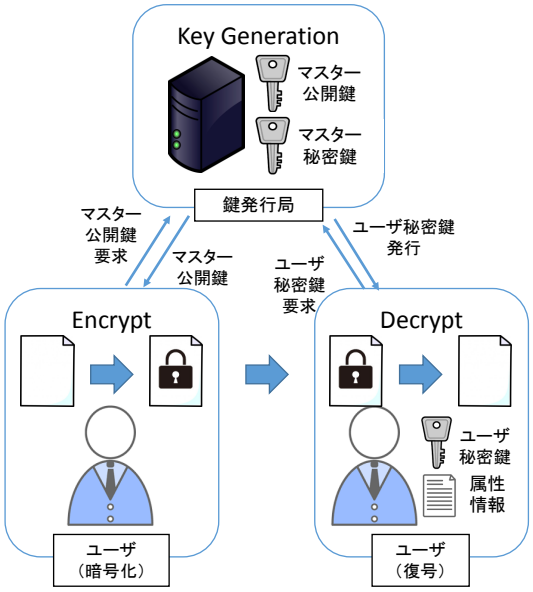

図 1　CP-ABE 概要

情報のフォーマット $\vec{n} := (d; n_1, ..., n_d)$ を入力とし，マスター公開鍵 PK とマスター秘密鍵 SK を出力する．

- Key Generation (PK, $\Psi := \{(t, \vec{x_t} := (x_{t,1}, ..., x_{t,n_t}) \in \mathbb{F}\backslash\{\vec{0}\} | 1 \leq t \leq d\}$):
  PK，SK および属性情報の集合 $\Psi := \{(t, \vec{x_t} := (x_{t,1}, ..., x_{t,n_t}) \in \mathbb{F}\backslash\{\vec{0}\} | 1 \leq t \leq d\}$ を入力とし，その属性情報の集合に対応するユーザ秘密鍵 SK_Ψ を出力する．
- Encrypt(PK, $\Upsilon := (M, \rho)$):
  マスター公開鍵 PK，復号に必要なアクセス構造 Υ および平文 M を入力とし，暗号文 ct_Υ を出力する．
- Decrypt(PK, ct_Υ, SK_Ψ):
  マスター公開鍵 PK，暗号文 ct_Υ，ユーザ秘密鍵 SK_Ψ を入力とし，$R(\Psi, \Upsilon) = True$ の関係が成立する場合にのみ，平文 M を復号する．

CP-ABE は鍵発行局を利用する必要がある．鍵発行局は Setup でマスター公開鍵 PK とマスター秘密鍵 SK を生成する．ユーザが Encrypt でマスター公開鍵 PK を用いて，復号条件を指定し平文 M を暗号化する．Key Generation はマスター公開鍵 PK とユーザの属性情報を利用して，鍵発行局が実行する．Decrypt は，ユーザの秘密鍵に関連付けられた属性情報が暗号文の復号条件を満たすとき実行可能である．

5. 提案システム

秘密分散法，属性ベース暗号，提案システムの比較を**表 1** に示す．提案システムでは，秘密分散法と属性ベース暗号を用いることで，秘密分散法の欠点を補っている．秘密分散法では，暗号化処理で生成した分散データのうちの閾値以上が必要という復号条件さえ満たせば，誰でも元のデータの復元が可能だが，提案システムではさらに属性ベース暗号の復号が必要で，元のデータへのアクセス権限のあるユーザしか復号を行うことができない．

表 1　各暗号手法の特徴

	秘密分散法	属性ベース暗号	提案システム
共謀への耐性	×	○	○
盗聴への耐性	×	○	○
ユーザ認証	×	○	○
データの冗長性	○	×	○

本章では，秘密分散法で暗号化されたデータを分散データ，属性ベース暗号で暗号化されたデータを秘密データと呼ぶ．

5.1 提案システムの構成

提案システムの構成を**図 2** に示す．ユーザはクラウドストレージサービスに保存したいデータを暗号化・復号処理サーバに送り，暗号化・復号処理サーバで秘密分散法の暗号化・復号処理と属性ベース暗号の暗号化処理を行う．属性ベース暗号の復号はデータを要求するユーザが行う．クラウドストレージとのデータの通信は暗号化・復号処理サーバが行う．クラウドストレージはデータの管理・保存を行う．ただし，単体のクラウドストレージに秘密分散法の暗号化処理の際に決定した閾値以上のデータが保存されることはないとする．属性ベース暗号で利用するマスター公開鍵とマスター秘密鍵は鍵発行局が生成し管理する．ユーザ秘密鍵も鍵発行局が生成し各ユーザに発行する．

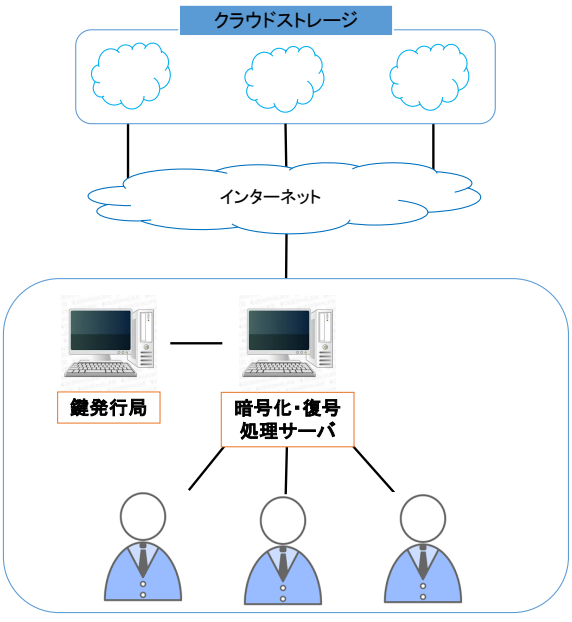

図 2　提案システム

5.2 信頼性

提案システムの信頼性について説明する．システムを利用する各ユーザは暗号化・復号処理サーバで属性ベース暗号の暗号化処理を行う前には盗聴などの不正な行為を行わないと信頼し，アクセス権限のないユーザが不正に元のデータにアクセスする可能性はないとする．ただし，暗号化処理を完了してからはアクセス権限があるユーザしか元のデータを手に入れることはできないため，各ユーザを信頼する必要はない．暗号化・復号処理サーバは暗号化・復号処理の際に不正な行為を行わず，また意図的なデータの漏えい等の行為を行わないと想定し信頼する．しかし，クラウドストレージサービスは，プロバイダによる保存しているデータの意図的な漏えいや不正な閲覧等の可能性があると想定し信頼しないものとする．外部の悪意のユーザによってクラウドストレージと暗号化・復号処理サーバ間は盗聴されると想定し信頼しない．鍵発行局と暗号化・復号処理サーバ間，ユーザと暗号化・復号処理サーバ間は盗聴されないと想定する．ただし，暗号化されているデータに関しては盗聴される可能性はあると想定し信頼しない．

5.3 暗号化

提案システムの暗号化処理の手順について説明する．提案システムでは秘密分散法と属性ベース暗号を用いた暗号化処理を行う．ただし，属性ベース暗号で利用するマスター公開鍵とマスター秘密鍵，各ユーザの秘密鍵の生成はすでに鍵発行局が終えているとし，以下の暗号化処理の手順には含まない．

暗号化処理

(1) ユーザがクラウドストレージに保存したいデータを暗号化・復号処理サーバに送信する．
(2) 暗号化・復号処理サーバが，マスター公開鍵を用いて属性ベース暗号による暗号化を行い秘密データを生成する．このときに復号条件を指定する．
(3) 暗号化・復号処理サーバが，(2) の秘密データを秘密分散法で暗号化し分散データを生成する．このとき閾値と分散数を指定する．
(4) 暗号化・復号処理サーバは，(3) の分散データを各クラウドストレージに送信する．

5.4 復号

復号処理の手順について説明する．暗号化処理と同様に，秘密分散法と属性ベース暗号を用いた復号処理を行う．ただし，属性ベース暗号の復号に必要な各ユーザの秘密鍵は，鍵発行局から各ユーザにすでに発行しているとし，以下の復号処理の手順には含まない．

復号処理

(1) クラウドストレージに保存されているデータを要求するユーザが，暗号化・復号処理サーバにデータを要求する．
(2) 暗号化・復号処理サーバは任意のクラウドストレージを選択し，分散データのうち閾値以上をダウンロードする．
(3) 暗号化・復号処理サーバは (2) でダウンロードした分散データを用いて秘密分散法の復号を行う．このとき閾値以上を集めることができた場合，秘密分散法の復号に成功する．集めることができなかった場合，復号に失敗する．
(4) 暗号化・復号処理サーバは (3) で生成した秘密データをユーザに送信する．
(5) ユーザは（4）で受け取った秘密データをユーザ自身の秘密鍵を用いて属性ベース暗号の復号を行う．ユーザの属性情報が属性ベース暗号の暗号化の際に指定した復号条件を満たす場合，復号に成功する．満たさない場合，復号に失敗する．

5.5 攻撃への耐性

提案システムの共謀・盗聴への耐性を前述の提案システムの信頼性に基づいて議論する．

5.5.1 共謀

データを管理しているクラウドストレージサービスプロバイダのうち，複数のプロバイダが協力して元のデータを手に入れようとしたと想定する．秘密分散法は暗号化で生成された分散データのうち，暗号化の際に決定した閾値以上のデータがあれば元のデータの復号が誰でも可能である．このことから，単体のクラウドストレージで管理されているデータが閾値以上ではなくても複数のプロバイダが協力すれば秘密分散法の復号が可能である．しかし，提案システムでは属性ベース暗号の復号も行わなければ元のデータを手に入れることはできない．属性ベース暗号の復号では復号条件を満たす属性情報に関連付けられたユーザ秘密鍵が必要となる．ユーザ秘密鍵は共有グループの各ユーザが管理しているので，複数のプロバイダが協力したとしても元のデータを手に入れることはできない．また，共有グループ内のデータへのアクセス権限のない複数のユーザが協力して，元のデータを復号しようとしたと想定する．この場合も複数のプロバイダによる共謀の場合と同様に，まず閾値以上の分散データを集め秘密分散法の復号条件を満たす必要がある．さらに，属性ベース暗号の復号の際に復号条件を満たす属性情報に関連付けられたユーザ秘密鍵も必要となる．アクセス権限のない複数のユーザが協力したとしても，属性ベース暗号の復号条件を満たすことはできないので，元のデータを手に入れることはできない．したがって，提案システムでは複数のクラウドストレージサービスプロバイダ，もしくは共有グループ内のデータへのアクセス権限のない複数のユーザが共謀したしても，元のデータを手に入れることはできない．

5.5.2 盗聴

外部から悪意のあるユーザによって暗号化を行ったデータを盗聴されたと想定する．このとき，秘密分散法で生成された分散データのうち閾値以上を集めなければ，秘密分散法の復号を行うことはできない．閾値以上の分散データを集め秘密分散法の復号に成功したとしても，属性ベース暗号の暗号化の際に指定した復号条件を満たす属性情報に関連付けられたユーザ秘密鍵を所有していなければ，元のデータを手に入れることはできない．次に共有グループ内のデータへのアクセス権限のないユーザが，共有グループのユーザと暗号化・復号処理サーバ間で盗聴を行い，秘密データを手に入れたと想定する．先ほどの想定と同様に，属性ベース暗号の復号条件をユーザ自身の秘密鍵が満たしていなければ，元のデータを得ることはできない．したがって，暗号化されたデータは盗聴されたとしても外部の悪意のあるユーザ，もしくは共有グループ内のアクセス権限のないユーザは元のデータを得ることはできない．

6. 実装

提案システムを実際の環境で実装した．今回の実装では，ユーザ，暗号化・復号処理サーバ，鍵発行局の機能を単一のPC に実装した．実装した PC のスペックを**表 2** に示す．クラウドストレージサービスは Dropbox，Box，OneDrive，Google Drive を利用した．秘密分散法は Ubuntu のパッケージで提供されている libgfshare-1.0.5 を利用し，CP-ABE は cpabe toolkit 0.11[11] を利用した．

システムの各構成要素の機能を**表 3** に示す．

表 2 実装環境

	ユーザ 暗号化・復号処理サーバ 鍵発行局
CPU	intel Core2 Duo 3.16GHz
メモリ	4GB
OS	Ubuntu 14.04

表 3 構成要素の機能

構成要素	役割
ユーザ	CP-ABE の復号 ユーザ秘密鍵の管理 暗号化・復号処理サーバとの通信
暗号化・復号処理サーバ	秘密分散法の暗号化・復号 CP-ABE の暗号化 ユーザとの通信 クラウドストレージとの通信
鍵発行局	マスター公開鍵の生成・管理 マスター秘密鍵の生成・管理 ユーザ秘密鍵の生成
クラウドストレージ	データの管理・保存 暗号化・復号処理サーバとの通信

表 4 計測時の各暗号手法のパラメータ

秘密分散法	閾値 k	10, 20, 30, 40
	分散数 n	50
CP-ABE	復号条件の属性数	10
	復号条件の論理式	and のみ，or のみ

7. 評価

本節では，提案システムの評価を行う．

7.1 処理時間の計測

実装したシステムが実用的であるかどうか評価するために，実際に暗号化・復号処理を行い処理時間を計測した．計測結果をもとに評価を行う．計測した際の秘密分散法と CP-ABE の各パラメータを**表 4** に示す．暗号化・復号処理を行った際の秘密分散法と秘密分散法の分散数 n は 50 に固定し，閾値 k の値は 10，20，30，40 で計測した．CP-ABE の復号条件の属性数は 10 に固定し，復号条件の論理式は and のみの場合と or のみの場合で計測した．CP-ABE の復号では復号条件の論理式が and のみの場合，or のみの場合どちらの条件も満たすユーザ秘密鍵を使用した．秘密分散法の閾値の値が大きいほど悪意のあるユーザが元のデータの復号することは困難だといえる．そこで時間計測では閾値の値を変化させ，処理時間がどれだけ変化するか確認した．処理で用いたデータのサイズは 1MB で計測した．

暗号化処理の計測結果を**図 3** に，復号処理の計測結果を**図 4** に示す．提案システムが実用的であるかどうか評価するために処理時間の計測を行った．

図 3 より，閾値 k の値に比例して暗号化処理の時間が増加しており，閾値の値が 10 増加するごとに暗号化処理の時間はおよそ 1.5 秒増加している．また，CP-ABE の復号条件が and のみの場合と or のみの場合で暗号化処理の時間にほとんど差はないことがわかる．

図 4 より，暗号化処理と同様に閾値の値に比例して復号処理の時間が増加していることがわかる．また，復号処理では CP-ABE の復号条件が and のみの場合と or のみの場合で処理時間に差があり，or のみの場合のほうが処理時間がおよそ 0.03 秒短くなっていることがわかる．このことから，CP-ABE の復号条件が and のみの場合は復号処理にかかる時間は増加するが復号条件は厳しくなるといえる．逆に or のみの場合は復号処理にかかる時間は短くなるが復号条件は緩くなるといえる．

図 3 と図 4 の比較から，暗号化処理に比べ復号処理にかかる時間は短いことがわかる．また，暗号化・復号処理ともに秘密分散法の閾値に比例して処理時間が増加していることから，閾値を大きくするほど処理時間は増加するが復号条件は厳しくなるといえる．逆に閾値を小さくするほど処理時間は短くなるが復号条件は緩くなるといえる．暗号

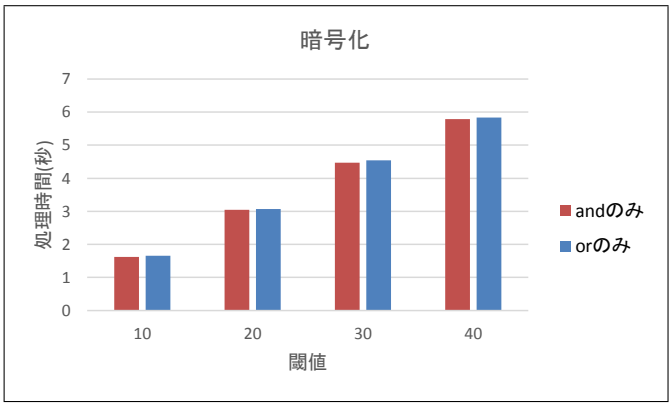

図 3　暗号化処理時間

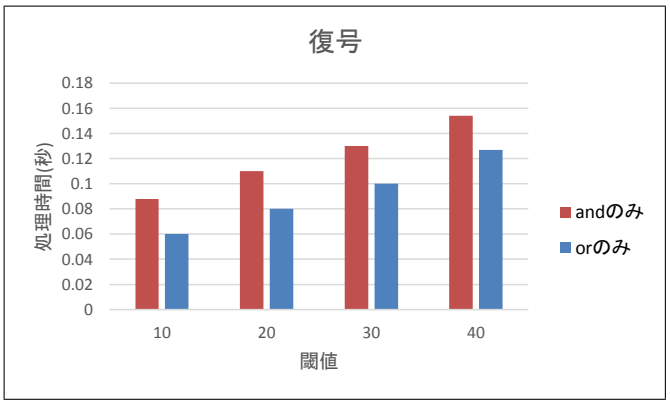

図 4　復号処理時間

化処理を行う頻度は復号処理を行う頻度に比べ低いことから，暗号化処理が復号処理よりも時間がかかったとしても大きな負担にはならないといえる．

8. 終わりに

本稿では，秘密分散法と属性ベース暗号を組み合わせたマルチクラウドストレージサービスのシステムを提案し，暗号化・復号処理の実装と評価を行った．

提案システムでは，クラウドストレージサービスのデータの漏えい等の機密性の問題を秘密分散法を用いることで解決した．また，秘密分散法を用いることで，ユーザに応じたアクセス制御やユーザ間でのデータの共有が困難であるという問題とクラウドストレージサービスプロバイダの共謀によるデータ漏えいの問題を属性ベース暗号を用いることで解決した．

今後の課題として，秘密分散法の暗号化・復号処理時間の高速化とストレージコストを軽減する必要性があると考えられる．本稿では取り上げなかったが，秘密分散法の高速化に関する研究 [12] やコストストレージの軽減に関する研究 [13], [14] が行われている．本稿で提案したシステムでも秘密分散法の高速化とコストストレージの軽減を行い，提案システムの改善を行う必要があると考えられる．また，クラウドストレージサービスとの通信を工夫し，提案システムの利便性を高める必要があると考えられる．各クラウドストレージサービスの通信速度に応じて動的に使用するクラウドストレージを選択し，通信時間を最適化するような手法が必要だと考えられる．

参考文献

[1] Cloud Security Alliance, “Cloud Control Matrix Version 3.0.1,” 2016.

[2] H. Sato, A. Kanai, S. Tanimoto, “A Cloud Trust Model in Security Aware Cloud,” Proceedings of 10th International Symposium on Applications and the Internet (SAINT 2010), pp.121–124, 2010.

[3] H. Sato, A. Kanai, S. Tanimoto, “Building a Security Aware Cloud by Extending Internal Control to Cloud,” Proc.10th Int’l Symposium on Autonomous Decentralized Systems (ISADS 2011), 323–326., 2011.

[4] A. Shemir. “How to share a secret,” Communications of the ACM, vol.22, no.11, pp.612-613 (1979).

[5] A. Sahai, B. Waters, “Fuzzy Identity-Based Encryption,” *EUROCRYPT,* Cramer, R. (Ed.), Lecture Notes in Computer Science, Vol.3494, pp.457-473, Springer (2005).

[6] A. Kanai, N. Kikuchi, S. Tanimoto, H. Sato, “Data Management Approach for Multiple Clouds using Secret Sharing Scheme,” 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp.432-437, 2014.

[7] 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．電子情報通信学会ライフインテリジェンスとオフィス情報システム研究会，2012.

[8] J. Bethencourt, A. Sahai, B. Watars, “Ciphertext-Policy Attribute-Based Encryption,” *IEEE Symposium on Security and Privacy*, pp.321-334, IEEE Computer Society (2007).

[9] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Effcient, and Provably Secure Realization,” Public Key Cryptography(PKC 2011). LNCS 6571, pp.53-70, March 2011.

[10] V. Goyal, O. Pandey, A. Sahai, B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc.ACM CSS, pp.89-98, October 2006.

[11] Advanced Crypto Software Collection, http://acsc.cs.utexas.edu/cpabe, 2016 年 8 月 9 日アクセス．

[12] 高荒亮 , 岩村恵市, “XOR を用いた高速な (k, L, n) ランプ型秘密分散法に関する研究,” コンピューターセキュリティシンポジウム 2009 B9-3, 2009.

[13] G. R. Blakley, “Security of ramp schemes,” Crypto’84, pp.242-268, 1984.

[14] 山本博資, “(k, L, n) しきい値秘密分散システム,” 電子通信学会論文誌, vol.J68-A, no.9, pp.945-952, 1985.