クラウドスケジュールサービスにおける日付偽装のための鍵共有方式の検討

横谷百合[†]　宮上達矢[†]　金井敦[†]
谷本茂明[†2]　佐藤周行[†3]

近年，新しい大規模分散処理システムとして知られている「クラウドコンピューティング」の普及が急速に進んでいる．しかし，クラウドサービスの管理者は信頼出来ない可能性もあり，セキュリティにおいて問題点がある．それ故，機密情報を扱う企業においてパブリッククラウドはあまり利用されていない．この問題に対応するために，これまでに，クラウドスケジュールサービスを例にとり，日付の偽装を行うことで，信頼できないクラウド管理者への対策を実現する方式・偽装アルゴリズムが提案されているが，アルゴリズム上必要となる日付偽装のための鍵は偽装と復号に同じ共通鍵を用いている．このため，このシステムを利用し複数人からなるグループでクラウドスケジュールサービスを共有しようとすると，偽装鍵も共有する必要があり，利便性に問題がある．これに対し，本論文では，秘密分散法を用いることにより，共有すべき偽装のための鍵を直接共有することなく，スケジュールサービスの共有をより容易に実現，管理する方式に関して提案し，有効であることを示す．

Calendar sharing with alteration method on public cloud

YURI YOKOTANI[†]　TATSUYA MIYAGAMI[†]　ATSUSHI KANAI[†]
SHIGEAKI TANIMOTO[†2]　HIROYUKI SATO[†3]

Cloud Computing has become more familiar. However, a cloud service administrator may be untrustworthy. Therefore it is difficult for companies dealing with confidential information to use a public cloud. In order to solve this problem, a data-alteration method has been proposed. It realizes preventing a leakage of private information from a cloud schedule service by using alteration algorithm with a key. In this paper, we propose sharing schedule data conveniently by using secret sharing system. Consequently, we can share the schedule data without sharing key of alteration directly, and easily management in the case of member management.

1. はじめに

近年，新しい大規模分散処理システムとして知られている「クラウドコンピューティング」の普及が急速に進んでいる．これらクラウドコンピューティングを利用し，様々なサービスを提供しているクラウドサービスの種類は多岐にわたるが，クラウドコンピューティングを社会基盤として利用する事を考える場合にはセキュリティに関しても考慮する必要がある[1]. 例えばクラウドサービスと管理している管理者が信頼出来るかどうか，クラウドサービスを利用しているユーザには直接判断できない[2].

この問題への対応策として，例えば，ファイルストレージとして利用可能なクラウドシステムでは，データを暗号化してパブリッククラウドに預けるという方式が採用されていることも多いが，企業においてパブリッククラウドでのスケジュールサービスは利用が少ない[3].

とくに個人としての利用において，広く普及しており非常に有用なサービスとして知られているクラウドスケジュールサービスは，仮に企業でそのまま利用した場合，各人によって入力された予定情報から企業に関する情報を読み取られる可能性があるという点がある．また，スケジュールサービスをそのまま暗号化して利用しようとすると困難な点が出現する．すなわち，スケジュールサービスにおいて重要な情報の一つである日付情報の暗号化による問題である．日付は，取りうる値の範囲が定まっている．このため，単に暗号化処理を行うとその範囲から外れてしまうため，この状態でサービスを利用しようとすると，クラウドスケジュールサービスが正しく動作しない可能性がある．

この問題に対応するため，クラウドスケジュールサービスへ日付情報を送信する際に日付の偽装を行うことで，信頼できないクラウド管理者への対策を実現する方式・偽装アルゴリズムが提案されている．[4]

この提案では，偽装のために鍵が必要になる．アルゴリズム上，鍵は偽装と復号に同じ共通鍵を用いている．

ここで，もし仮にこの方式を利用したスケジュールサービスを複数人からなるグループで共有する場合，偽装に用いる鍵をグループ内のメンバ全員で共有する必要がある．同じ鍵をメンバで共有するということは，鍵が漏洩した場合にすべての情報が読み取られてしまうことや，メンバが増えると，その増加に比例して鍵を配布する準備の手間が増えること，脱退するメンバから鍵を回収しなければならないなど，デメリットも多く，その共有の方法に関しては考慮すべき点が多く存在する．　そこで，本論文では，情報を分割し，一つの情報をそれぞれ違う場所で管理するこ

とが可能である秘密分散法を用いることにより偽装のための鍵を直接共有することなく，スケジュールサービスの共有をより容易に実現, 管理する方式に関しての提案を行う．秘密分散法については複数の方式が提案されているが，(k,n)しきい値秘密分散法[5][6]を利用する．

2. 前提とする日付偽装方式

2.1 クラウドスケジュールサービスについて

クラウドスケジュールサービスとは，予定に関する情報をパブリックなクラウド環境に保存することでインターネット通信を通じてその予定を自由に閲覧・書込ができるサービスである．代表的なものには Google や Yahoo!によって提供されているものがある．予定に関する情報とは，予定が実施される年月日，時間帯，実施予定場所，予定の内容のことである．とくに，この中で予定が実施される年月日を日付情報と呼ぶ．

クラウドスケジュールサービスを 1 人で利用する場合には，自身のクラウドサービスにおけるアカウントからスケジュールサービスを利用するための認証を行い，サービスの提供を受ける．そしてその後予定に関する情報の入力，削除，閲覧などの処理をおこなう．

また，ここでは，パブリッククラウドは信頼出来ないものとする．それに伴い，パブリッククラウド側で管理されているサービス認証に用いるユーザ ID, パスワードなども同様のものとする．

2.2 日付の偽装について

ここでは，本稿において前提とされる日付偽装方式について述べる．

まずは予定情報を書込, 送信したい場合について述べる．ユーザには事前にスケジュールサービスに書込を行いたい予定情報があるとする．ここで，クライアント側であらかじめ用意したユーザパスワードを用いて日付偽装を行うための乱数を生成．これを偽装用の鍵とし，クライアント側で保存する．この鍵によって日付の偽装を行い，その結果として年月日がそもそもの予定と異なるものに偽装された日付情報を得る．その結果のみを，ネットワークを通じてスケジュールサービスへと送信することで，クラウド業者側には偽装前の日付を読み取ることができなくなる．

続いて，日付情報を読み出す場合は，偽装されている情報をダウンロードして，復号処理を行うことによって予定を読み込むことができる．

以下にシステムの動作を示した図を図 1 として示す．

尚，このモデルは 1 人でスケジュールサービスを利用する場合の状況を想定している．

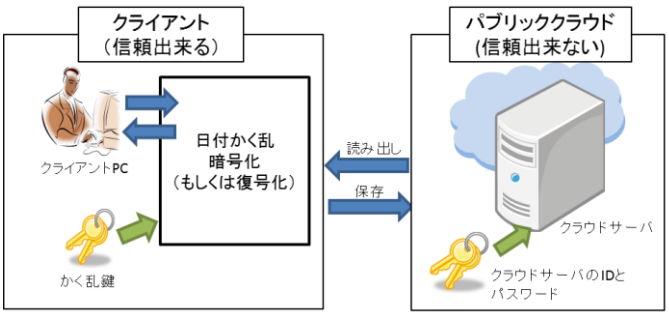

図 1 日付偽装方式の概念図

3. グループで共有する場合の要件

3.1 偽装鍵の共有上の問題

本稿では，偽装方式を用いて，それを複数人からなるグループで共有する場合に関して検討を行う．

この方式を利用する際には偽装に用いるための鍵が必要となる．また, 偽装と復号に同じ鍵を用いている．つまり，グループで共有する場合には，メンバ全員で一つの鍵を共有する必要があるということになる．

ここで，グループで一つの鍵を共有するという点において，いくつか課題となる点が存在する．ひとつは，全員で偽装用の鍵を直接的に共有してしまうと，誰かひとりからその鍵が漏洩，あるいは盗まれてしまった場合すべての情報が読み取られてしまうという問題である．このような状況が想像できるので，基本的に同じ鍵を全員で共有するというのに抵抗感がある場合もある．他にも，グループのメンバが加入／脱退した場合に鍵を新たに配布するという処理や，脱退後そのメンバがもつ鍵を使えないようにしなければならないなど，管理・運用の問題がある．

3.2 本提案で想定する利用法

なお，本提案では，あるグループがスケジュールサービスを共同使用する場合において，以下のような利用シーンを想定する．

まず利用開始時には，グループのリーダーとなる人物がスケジュールサービスの利用を開始，そのサービスへ同グループの各メンバを登録・招待する形で共有をはじめる．メンバはサービスのアカウントを事前に持っていることとする．ここで，あるグループを Gr とし，リーダーとなる人物が必ずひとり居ることとする．なお，リーダーがメンバのメールアドレスを登録することによって，登録されたメンバ以外はスケジュールが閲覧できないよう公開範囲を制限することができる．また現在実際に提供されているスケジュールサービスによっては，メールアドレスを登録する際に予定の閲覧・書込に関して細かな権限を設定することも可能であるが[7][8][9]，今回はグループのメンバは全員予定の閲覧・書込が自由に行えるものとした．

その後リーダーは日付を偽装するための鍵を生成し，本提案に沿って秘密分散法を用い，分散情報をそれぞれ配布する．メンバはそれぞれ自身の鍵となる分散情報を受け取ったのち，各自の PC から閲覧のためのアプリケーションを利用してスケジュールサービスにアクセスし，予定の閲覧・書込の処理を行う．このアプリケーションは，クラウドスケジュールサービス上に保存してある偽装されている予定情報を信頼できるローカルへダウンロードし，復号の処理を行うものであり，またそのために必要な事前処理も，アプリケーション内部で行うものとする．尚，グループに関しては，利用開始後に新たなメンバの加入，既存のメンバの脱退が可能であるが，それほど頻繁にメンバの入れ替えは起こらないものとする．

4. 本提案について

4.1 スケジュールサービス利用開始時

4.1.1 基本となる概念

３．１で指摘した問題点に対応するために，本方式では，メンバが n 人であるグループ Gr がすでに存在している状態で，n 人のうちのひとりであるリーダーが偽装用の鍵を用意する．その後，しきい値秘密分散法を用いて情報の分割を行う．なお，しきい値と分割する数を，(2 , n+1)とする．つまり，偽装用の鍵を n+1 個へ分割し，２つの分散情報が揃えば復元可能であるとする．分散情報のうち一つをグループ用の鍵として K_{Gr}，残りの n 個に関してはメンバに１つずつ異なる分散情報を配布する．

以降分割後の情報は K とアルファベットの添字によって表現することにし，Gr のリーダーを A とする．例えば Gr のメンバへ渡す分散情報は一人目から順に K_A，K_B，K_C, …となる．

4.1.2 分割した情報 K_{Gr} について．

偽装鍵 Key を分割した後にできた分散情報 K_{Gr} については，スケジュールサービスに１対１対応できるように紐付けし公開する．具体的にはスケジュールサービスの提供しているファイル添付機能の利用や，スケジュールを区別する ID や URL を利用し独自に用意を行こも可能であると考える．こうすることで，サービスへ登録されている各メンバは K_{Gr} へネットワークを通じて自由にアクセスできるようになる．

4.1.3 偽装鍵分割後の分散情報についての配布

K_{Gr} を除いた n 個の分散情報は n 人の各メンバにそのまま配布を行う．各メンバが受け取った後，この分散情報は各人の PC にあらかじめ入っているアプリケーション内で保管され，メンバが直接分散情報に関して操作を行うことはない．そして，アプリケーションにあらかじめ設定してあるユーザパスワードによって暗号化を施し情報そのものには容易にアクセスできないようにしておく．このアプリケーションに関しては後述する．また、偽装鍵に対して秘密分散法によって処理を行い，それぞれの分散情報を配布する様子を図 2 として以下に示す．

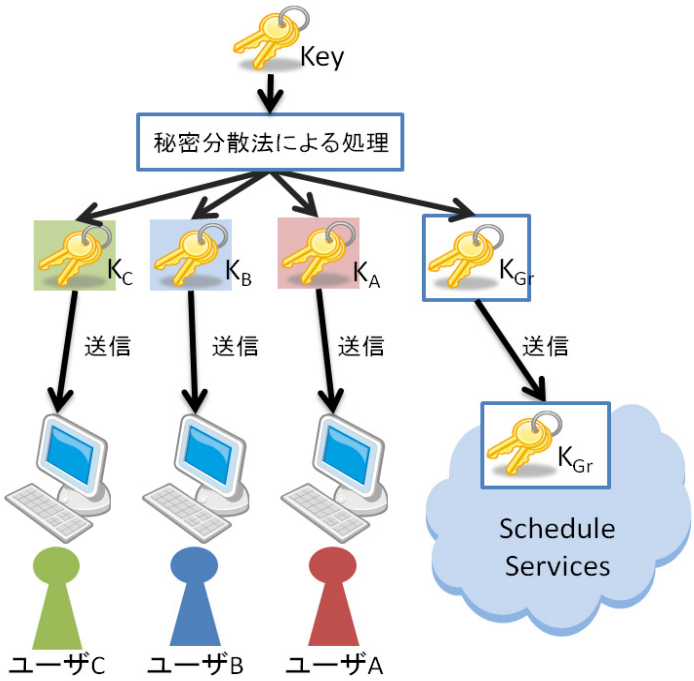

図 2 偽装鍵 Key の分散処理と配布の様子

4.2 サービス利用時に関して

4.2.1 アプリケーションの利用手順

前提となる利用条件においても触れたが，クラウドスケジュールサービス上にはすべて偽装された内容がアップロードされているため，実際メンバが情報を閲覧する際には独自のアプリケーションを利用することとなる．

このアプリケーション内部において，偽装されている予定情報の復号処理を行う．クラウドサービスへのログイン完了後に K_{Gr} の取得と偽装されている予定情報の入手をクラウドサービスに対して行うことと，ユーザパスワードによって保管されている K_A を取り出し K_{Gr} と共に Key を復元する処理を行う．その後，その Key を利用して閲覧・書込を行う．なお，一定の処理が完了したのち，K_{Gr} はアプリケーションから削除され，次回利用する場合にはもう一度同じ場所から取得する．こうすることで，復元された偽装鍵はメンバのローカル PC 内部に一時的にしか存在しないため，後からメンバ以外の人物がその鍵を利用することは困難になる．

4.2.2 メンバの途中加入時

グループ Gr に中途加入者 D が現れた場合には，Key から分割する分散情報の総数が異なるため，秘密分散法を用

いて処理を再度行う必要がある．もう一度秘密分散法による処理を行った後に K_{Gr} を新しいものに上書きし，各メンバ用の分散情報に関しても再配布を行い古いものに関しては破棄とする．だが，メンバの増減が頻繁に起こらないようであれば，あらかじめ多めの数で分割処理を行なっておいて，中途加入者へその都度配布するという形式を取ることも可能である．

4.2.3 メンバの途中脱退時

脱退時も，Key から分割する分散情報の総数が変化するため，秘密分散法を用いて再度処理を行う．その後，新しくなった K_{Gr} と脱退メンバを除いた個数の鍵をそれぞれ配りなおす．ここで K_{Gr} が新しい物に更新されると，今までの分散情報では Key の復元が不可能となる．例えばグループのメンバ B が脱退する場合には，B は分散情報である K_B を破棄するだけで良く，もし仮に B が分散情報を破棄しなかった場合でも K_{Gr} は新しい物に変わってしまっているため，偽装鍵を復元することはできなくなる．

4.3 システムを含めた全体的な構成について

クラウドスケジュールサービスとメンバを含めた，本方式に必要とされるシステムの全体的な構成について概念図を図３として以下に示す．クラウドスケジュールサービス上には，偽装された情報とメンバ全員が参照できる K_{Gr} が設置してある．メンバ A～C のローカル PC にはそれぞれアプリケーションが存在し，メンバはアプリケーションを通してスケジュールサービスへアクセスし予定情報の閲覧・書込を行う．図中ではメンバ A に関して注目しているが，他のメンバに関しても同様である．ただし，アプリケーション内部で保存される分散情報はメンバごとに異なっている．

5. 評価と考察

本方式が利用の際の管理やメンバの途中加入・脱退時に効率的であるのか評価を行うために，PKI（Public Key Infrastructure，公開鍵基盤）を利用し偽装鍵を共有したケースを想定し，その方式を利用した場合と本方式を利用した場合の利用手順や鍵を配布するリーダーの作業に関して比較を行うこととした．

5.1 PKI を利用して偽装鍵を共有した場合

PKI を利用し偽装鍵を各メンバへ配布した場合について，(1)スケジュールサービスの利用開始時，(2)通常利用時，(3)メンバの加入時，(4)メンバの脱退時に関して比較を行う．

PKI とは信頼出来る第三者による審査を受けることで利用者の身元に関して保証する仕組みのことであり，その結果利用者は信頼出来る第三者に認証された公開鍵と，その対を成す秘密鍵を所持していることになる．

偽装アルゴリズムを利用したクラウドスケジュールサービスの共有を行うとすれば，偽装用の鍵を各メンバのもつ公開鍵によって暗号化し，対応する各メンバにそれぞれ配布をするという流れになる．これに関して図４として示す．その後，各メンバが自身のみが知る秘密鍵で復号化を行い，偽装用の鍵を得ることになる．

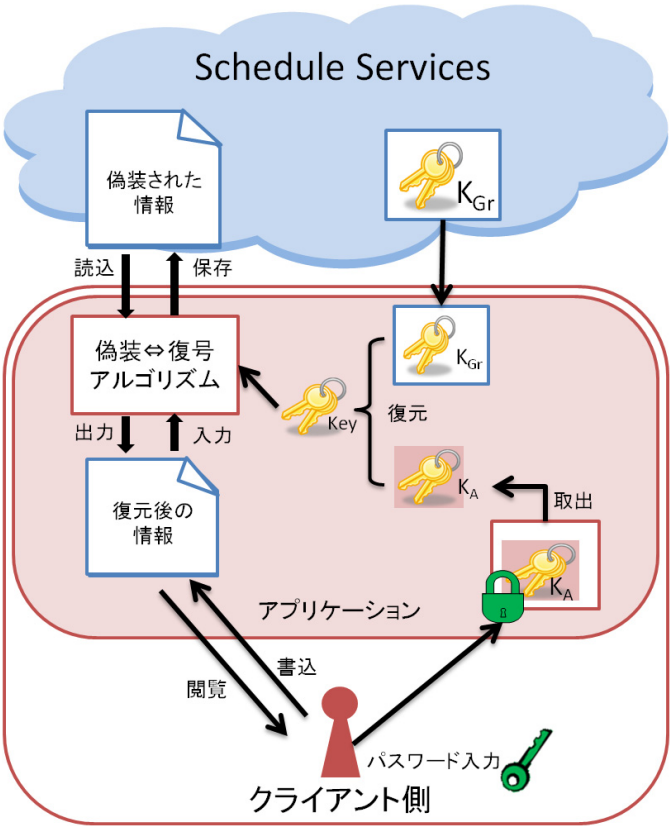

図 3　全体の概念図

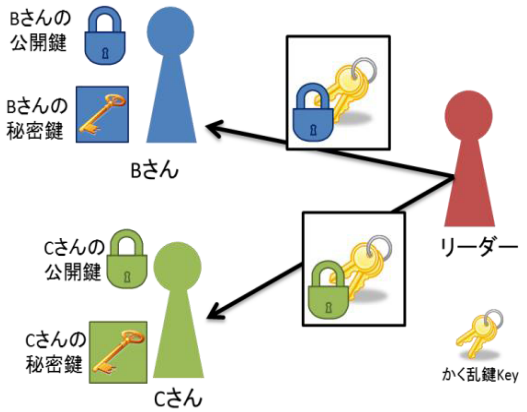

図 4　PKI 利用時のかく乱鍵配布

(1)スケジュールサービス利用開始時

利用開始時において，PKI を利用した場合は偽装鍵 Key を各メンバの公開鍵によって暗号化処理をし，対応する各メンバに対して送信する必要がある．また，PKI の制度を

利用しておらず，ユーザ独自の公開鍵と秘密鍵のペアを持たないメンバも存在する可能性がある．このメンバに対して鍵を配布する際には，メンバに PKI の制度を利用するよう申請してもらうか，偽装用の鍵を直接手渡しするなどして特別な配慮を行う必要がある．

対して，本方式では，秘密分散法によって分散処理した情報においては暗号化の処理をせずに送信しても直ちに偽装鍵 Key が盗まれる可能性は低いため，リーダーは暗号化処理の手間を軽減することができる．また，PKI に参加していないメンバに関しても事前の手続きや手渡しなどの特別な配慮が不要で，クラウドスケジュールサービスを共有するグループへ加入させることが可能である．

(2)通常利用時（閲覧・書込）

メンバが閲覧や書込を行う段階では，基本的にメンバが直接偽装鍵 Key を操作する必要がないように，同様のアプリケーションを利用することを想定している．

PKI 利用の場合は，メンバ自身の秘密鍵がそのままユーザパスワードの代わりになり，本方式の場合はアプリケーション独自のユーザパスワードをメンバに設定してもらい安全に保管する仕組みを利用する．

ただし，これらはすべてアプリケーション内部で行うため，メンバに必要とされるのは秘密鍵かユーザパスワードを入力しアプリケーションを起動させるという共通の手順のみである．メンバが利用する上で大きな違いはないといえる．

(3)メンバの加入時

グループ Gr に中途加入者 D が現れた場合には，PKI を利用すると，偽装鍵 Key を新しいメンバの公開鍵で暗号化し送信するだけで済む．しかしながら本方式では Key から分割する分散情報の総数が異なるため，秘密分散法を用いての処理を再度行う必要がある．だが，メンバの増減が頻繁に起こらないようであれば，あらかじめ多めの数で処理を行なっておいて，中途加入者へその都度配布するという形式を取ることもできるので，一度に沢山の途中加入者が現れない限りはあらかじめ用意しておいた分散情報で対応することが可能であるといえる．

(4)メンバの脱退時

メンバの脱退に関しては，メンバが脱退後にその資格を失ってからもスケジュールサービス上のデータを閲覧できてしまう可能性があるのは好ましくない．

PKI 利用の場合では，偽装鍵 Key 自身を既に配布しているため，Key そのものの変更が必要となってくる．そして Key が変更されるということは，クラウドスケジュールサービス上に保存してあるすべてのデータもまた新たに偽装し直す必要があるということである．この場合ではその上，新しい Key に関して再び各人の公開鍵を利用して配布していかなければならない．

一方，本方式では偽装鍵 Key を再度処理し，K_{Gr} と各人が保存すべき分散情報をそれぞれ配布し直す手間のみで，脱退後のメンバによるデータの閲覧を拒否することができる．

5.2 本方式との差異

PKI 利用時と本方式を比較すると，クラウドスケジュールサービスの共有を開始する際は，各メンバに配布すべき分散情報をそのまま配布できるため，PKI 利用者ではなく自身の公開鍵と秘密鍵のペアを持たないメンバに関しても特別な手段や例外の処理を必要とせず参加ができるという管理上の負担の軽減が見込まれる．

また実際メンバがアプリケーションを通じて利用する際に関しては，どちらのケースも偽装された予定情報を取得し復号化するのはアプリケーション内部が行うため，各メンバが普段利用する際やるべき操作というのは基本的に差異がないと言える．

そしてメンバが脱退する際に行わなければならない管理上の操作に大きな差が出る．時間が経過すればするほどクラウドスケジュールサービスに保存されているデータの総量も自然と増える．PKI を利用した場合には，そのデータをメンバが脱退するたびに偽装し直す必要があるが，これはグループで共有する上で管理の手間となり，管理を担当するリーダーへの直接的な負担となってしまう．一方，本方式では Key そのものを配布しない上に，Key を変更せずに秘密分散の処理を再度行うことで各メンバの持つ分散情報を変更することができる．これによって，クラウドスケジュールサービス上に保存してあるデータに関して再偽装の処理を行わずに，脱退したメンバからスケジュール閲覧の資格失効を実施することができる．つまり，本方式によって，共有されているスケジュールサービスを管理・運用の作業数が軽減できるといえる．

メンバが増加する際，秘密分散の処理を行わなければならないという点においては増加したメンバの公開鍵で暗号化し配布すれば済む PKI と比較しても管理上の手間となる部分が増えるが，あらかじめ余分に分散情報を用意しておくなど，工夫によってはある程度手間の軽減が可能になるのではないだろうか．

6. おわりに

本論文では，クラウドスケジュールサービスにおける日付偽装手法を利用した上でスケジュールサービスをグループで共有するための偽装鍵共有方式に関して検討し，秘密分散法を用いて実現する手法について提案をした．

この手法により第三者からの重要な予定に関する情報を

偽装した状態で，クラウドサービスのメリットの一つでもある，グループによるサービス共有を実現し，更に管理上の作業を軽減することが可能になったといえる．

今後この提案において，偽装のための鍵を秘密分散法によって処理する際の計算量に関して検討を行なっていく必要があると思われる．分割する元の情報の大きさや，分割する個数によってどのようになるのかを確認することで，PKI を利用し暗号化処理する処理との比較がより具体的に行えることになり，この方式の利便性を検証できるのではないだろうか.

参考文献

1) Carl Almond, “A Practical Guide to Cloud Computing Security ”, Accenture and Microsoft, August 27, 2009

2) “Public Cloud Computing Security Issues” , http://www.thebunker.net/managed-hosting/cloud/public-cloud-computing-security-issues/ ,

3) Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, and Tangs Chaojing, , “Data Security Model for Cloud Computing” , ISBN 978-952-5726-06-0, Proceeding of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22 2009

4) 宮上達矢，”Alteration Method of Schedule Information on Public Cloud for Preserving Privacy” , The Sixth International Conference on Digital Society (ICDS 2012) , February 2012.

5) Shamir Adi, “How to share a secret”, Comm. Assoc. Comput. Mach. , vol.22, no.11 , pp.612-613(Nov. 1979)

6) "注目の情報管理方式「しきい値秘密分散法」", http://www.atmarkit.co.jp/fsecurity/special/53tsss/tsss.html

7) “特定のユーザとカレンダーを共有する - Google カレンダーヘルプ , http://support.google.com/calendar/bin/answer.py?hl=ja&answer=37082

8) “Yahoo!グループヘルプ- カレンダー機能ヘルプ” , http://help.yahoo.co.jp/help/jp/groups/calendar/

9) “iCloud: カレンダーまたはリマインダーリストをほかの人と共有する”, http://support.apple.com/kb/PH2690?viewlocale=ja_JP&locale=ja_JP