

# 多対多の暗復号化可能な秘密計算プロトコルの提案

坂崎 尚生<sup>1</sup> 安細 康介<sup>1</sup>

**概要:** 本研究では、高額医療・高額介護合算療養費制度等における「自己負担額の世帯合算および現物給付サービス」の仕組みを電子的に実現する方法について、セキュリティ面からの検討を行う。

より具体的には、暗号化状態まま計算が可能な秘密計算と呼ばれる技術を上記仕組みに適用する為の要件を定義し、その要件を満たす秘密計算プロトコルを提案する。

**キーワード:** 秘密計算, Paillier 暗号, 高額医療・高額介護合算療養費制度, 総合合算制度, 現物給付

## Proposal of Secret Computation Scheme corresponding to Many-to-many Encryption and Decryption.

HISAO SAKAZAKI<sup>1</sup> KOUSUKE ANZAI<sup>1</sup>

**Abstract:** We define the application requirements to the high-cost medical expense benefit system of secret computation technology. In addition, we propose a secret computation method that meets the requirements.

**Keywords:** secret computation, Paillier encryption, high-cost medical expense benefit system, benefit in kind.

### 1. はじめに

2008年4月1日より始まった高額医療・高額介護合算療養費制度は、世帯内の同一の医療保険の加入者について、毎年8月から1年間にかかった医療保険と介護保険の自己負担を世帯合算し、基準額を超えている場合は、加入している医療保険の窓口申請することにより、その超えた金額を受け取ることができる現金給付型の制度である<sup>\*1</sup>。

また、2015年10月に政府与党により見送りになってしまったが、医療費と介護費だけでなく、障害・保育に係わる費用も世帯合算させる総合合算制度の導入も検討されていた[5]。総合合算制度では、マイナンバー等を利用して患者が支払った医療費等の自己負担額を集計し、医療機関

等が該当者の世帯合算値を確認することにより、基準額に達した患者は、受診時の窓口負担をしなくても済む現物給付型のサービスも検討されていた。

本研究では、高額医療・高額介護合算療養費制度または総合合算制度における現物給付型サービスの電子化に向けて、その核心となる「自己負担額のオンライン集計」および「世帯合算値のリアルタイム確認<sup>\*2</sup>」の仕組みを、主にセキュリティの面より検討を行った。

より具体的には、自己負担額の情報等は、個人のプライ

<sup>1</sup> (株)日立製作所 研究開発グループ  
システムイノベーションセンタ

Hitachi, Ltd., & Development Group,  
Center for Technology Innovation - Systems Engineering

<sup>\*1</sup> 高額医療・高額介護合算療養費制度では、事前に全国健康保険協会の各都道府県支部から健康保険限度額適用認定証を取得し、医療機関に同認定証を提出することにより、受診時の窓口負担をしなくても済む現物給付型のサービスも受けることができる。

<sup>\*2</sup> 政府検討資料[5]では、医療機関等のサービス事業者が該当者の世帯合算値を確認する具体的な方法については明記されていない。つまり世帯合算値を確認する具体的な方法として、サービス事業者が集計された情報を管理しているサーバにアクセスして、リアルタイムに世帯合算値の確認を行うのか、または、現状の高額医療・高額介護合算療養費制度の現物給付型サービスの様に、利用者が予め取得した限度額適用認定証をサービス事業者に提出することで確認させるのかまでは、明記されていない。

しかし、マイナンバー制度の目的の一つとして「添付書類の削減」を掲げていることから、現物給付型サービスの将来像としては、前者の仕組みの方が望ましいと考える。それ故、本研究では、医療機関等のサービス事業者がリアルタイムで該当者の世帯合算値を確認する仕組みをあるべき姿とし、その仕組みを実現する上でのセキュリティに関する検討を行った。

バシーに係わる情報であるので、上記仕組みを実現する上では、それらの情報をより安全に集計し、より安全に世帯合算値を確認できるようにする必要がある。

そこで、本研究では、暗号化状態まま算術演算をすることができる秘密計算と呼ばれる技術 [1][2][3] に着目し、自己負担額を暗号化したまま世帯合算値を求める方法を検討した。

秘密計算技術を上記仕組みに適用する上で、我々は、まず、「自己負担額のオンライン集計」および「世帯合算値のリアルタイム確認」の仕組みのモデル化を行った。また、そのモデルに従い、上記仕組みに求められるセキュリティ要件を定義した。

そして、そのセキュリティ要件と既存技術 [1][2][3] とを照らし合わせ、秘密計算技術を我々のモデルに適用する上での課題を整理した。

最後に我々は、その課題を解決する為に、既存技術 [1] を改良し、全てのセキュリティ要件を満たす秘密計算プロトコルを設計した。

本論文の構成は次の通りである。2章では医療費等合算制度の電子化に向けた提案モデルとセキュリティ要件について説明する。3章では秘密計算技術を提案モデルに適用する上での課題を説明する。4章にてセキュリティ要件を満たす秘密計算プロトコルを提案し、5章にて本論文を纏める。

## 2. 提案モデルとセキュリティ要件

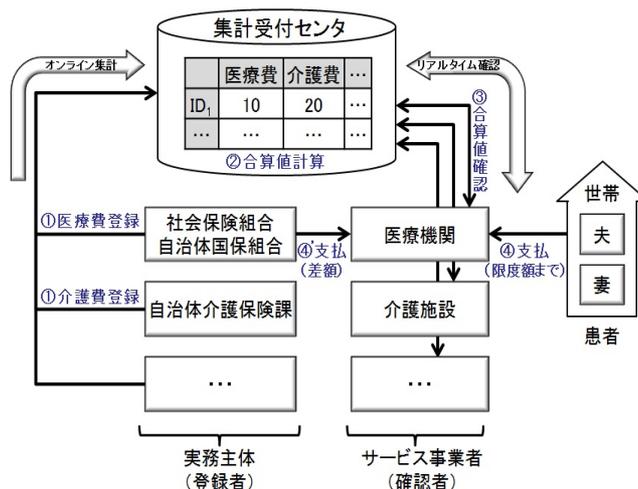
### 2.1 提案モデルの概要

我々は、まず、「自己負担額のオンライン集計」および「世帯合算値のリアルタイム確認」の仕組みのモデル化を行った。本節では、我々が提案するモデルについて説明する(図1参照)。

提案モデルのステークホルダは、以下である。

- 実務主体（登録者）：医療費制度や介護費等制度等の実務を行う者。医療費制度における社会保険組合や自治体の国保組合、介護費制度における自治体の介護保険課などがこれに当たる。現状、実務主体は、レセプト等の診療報酬明細書より、個人が支払った医療費や介護費等を把握しており、それらの情報は各々の実務主体によって管理されている。本モデルでは、図1①の様に、実務主体が本人に代わって個人が支払った医療費や介護費等の情報を集計受付センタに登録する。
- 集計受付センタ：クラウド上のデータセンタ。各実務主体から送られてきた医療費や介護費等の個人支払情報を収集し、世帯毎の合算値を計算する(図1②)。また、サービス事業者からの確認依頼に応じて、該当者の自己負担額の世帯合算値をサービス事業者へ通知する。

図1 提案モデル



- サービス事業者（確認者）：医療や介護等のサービスを行う医療機関や介護施設等。診療費を患者に窓口請求をする際、集計受付センタに該当者の世帯合算値を確認し(図1③)、その限度額までを患者に窓口請求する。尚、診療費と窓口請求額とで差が生じた場合、サービス事業者は、その差額を実務主体に請求し、実務主体の保険料より支払われる(図1④)。
- 患者：医療や介護等のサービスを受ける者。サービス事業者が算出した窓口請求額を支払う(図1④)。

提案モデルでは、複数の実務主体（登録者）がデータを集計受付センタに登録し、複数のサービス事業者（確認者）が集計受付センタに問い合わせた該当者の世帯合算値を確認する、というのが特徴である。

### 2.2 セキュリティ要件

本節では、前記モデルをベースとして、実務主体、集計受付センタおよびサービス事業者が果たすべきセキュリティ要件を定義する\*3。

【要件1】実務主体は、個人が支払った医療費や介護費等の情報を集計受付センタに登録することが主な役割である。医療費や介護費の支払情報は、個人のプライバシーに係わる情報であるので、実務主体は、それらの情報を外部に漏らすことなく、安全に集計受付センタに登録しなければならない。

【要件2】集計受付センタは、世帯合算値を計算し、サービス事業者へ通知することが主な役割である。集計受付センタ自身は、実務主体から送られてくる個々のデータの値や世帯毎の合算値を知る必要はない。役所等の

\*3 ステークホルダの内、患者に対しては、IoTシステムを直接触れる訳ではなく、サービス事業者が算出した窓口請求額を支払うだけなので、ここではセキュリティ要件を求めないとする。

職員が興味本位に個人情報不正閲覧するような事件が多発する状況 [7][8] を鑑みると、知る必要のない情報は、例えば集計受付センタの運用者や管理者でも、閲覧できない仕組みにしておくのが望ましい。また、2009年に起きた米国クレジットカード漏洩事件 [9] では、加盟店との通信を SSL で暗号化していたにもかかわらず、カード会社のサーバ上で復号された瞬間をウイルスにより搾取されクレジットカード情報が漏洩している。このようなウイルス対策という観点からも、個人情報が集まる集計受付センタでは、個人情報を平文のまま管理せず、常に暗号化して管理する等の安全対策を施しておくことが望ましい。

【要件 3】サービス事業者は、集計受付センタに該当者の世帯合算値を確認し、その限度額までを患者に窓口請求を行う。提案モデルでは、サービス事業者は複数存在し、各々、該当者の世帯合算値を取得できなければならない。しかし、十分な安全管理が行えるサービス事業者からそうでないサービス事業者まで存在する。それ故、あるサービス事業者からの情報漏洩事故が、システム全体に波及しない仕組みにしておく必要がある。(例えば、全サービス事業者にシステム共通の秘密鍵を配布するような仕組みにはならない。)

本研究では上記 3 つを、提案モデルを安全に実現する上でセキュリティ要件として定義した。

### 3. 既存技術の適用上の課題

我々の目的は、2章で定義したセキュリティ要件を満たすシステムの構築である。

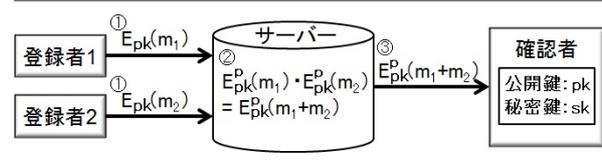
データの機密性を確保する一般的な方法として、データの暗号化がある。特にクラウド等のデータセンタを中継してデータが送受信される場合には、データの送信者から受信者までを End-to-End で暗号化をすることにより、データセンタでの不正閲覧やデータセンタに仕掛けられたウイルスによる情報漏洩事故を防ぐことができる(要件 1,2 対応)。

一方、提案モデルでは、集計受付センタは、サービス事業者の依頼に応じて、該当者の世帯合算値を計算する必要があり、End-to-End で個々のデータが暗号化されてしまうと、集計受付センタでは個々のデータから合算値を計算することが難しくなる。

そこで、本研究では、暗号化状態まま算術演算をすることができる秘密計算と呼ばれる技術 [1][2][3] に着目し、自己負担額を暗号化したまま世帯合算値を求める方法を検討した。

暗号理論では古くから入力データを秘匿しつつ、正しい値になるように計算をすることができる秘密計算の研究が進められており、加法準同型暗号に基づく Paillier 暗号 [1]

図 2 一般的な Paillier 利用モデル



や乗法準同型暗号に基づく RSA 暗号 [2] などが知られている。また、最近では、Craig Gentry により完全準同型暗号に基づく方式 [3] \*4 が提案されている。

秘密計算技術は、ここ近年、パーソナルデータを扱う際の情報漏洩を防ぐ技術として期待されてきている [6]。

本研究では、自己負担額の世帯合算値を安全に計算することが目的であるので、既存技術の内、暗号化状態で加法を行うことができる Paillier 暗号 [1] の適用を試みた。

#### 3.1 Paillier 暗号

まず、準備として、Paillier 暗号 [1] について説明する。尚、本論文では公開鍵  $pk$  での Paillier 暗号化関数を  $E_{pk}^p()$  と表記し、秘密鍵  $sk$  での Paillier 復号関数を  $D_{sk}^p()$  と表記する。

Paillier 暗号は Pascal Paillier が 1999 年に提案した公開鍵暗号方式であり、合成数剰余判定仮定の下で加法準同型性を持つ IND-CPA 安全な方式である。

Paillier 暗号では  $n = p \cdot q$  ( $p, q$  は素数) とする。また、 $k \in \mathbb{Z}_n^*$  を任意に選び、 $g = 1 + k \cdot n \pmod{n^2}$  とする。そして、 $pk = (n, g)$  を公開鍵とし、 $sk = (p, q)$  を秘密鍵とする。この時、平文  $m$  の暗号化は以下である。

$$c = E_{pk}^p(m) = g^m \cdot r^n \pmod{n^2}.$$

尚、 $r \in \mathbb{Z}_n^*$  は任意の乱数である。

また、暗号文  $c$  の復号化は以下である。

$$m = D_{sk}^p(c) = \frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} \pmod{n}.$$

尚、 $\lambda = \text{lcm}(p-1, q-1)$  であり、 $L$  は以下である。

$$L(x) = \frac{x-1}{n} \pmod{n^2}.$$

Paillier 暗号の特徴は、加法に関して準同型の性質を持つことであり、平文  $m_1, m_2$  に対して以下が成り立つ。

$$\begin{aligned} E_{pk}^p(m_1) \cdot E_{pk}^p(m_2) &= E_{pk}^p(m_1 + m_2), \\ E_{pk}^p(m_1)^{m_2} &= E_{pk}^p(m_1 \cdot m_2). \end{aligned}$$

一般的に Paillier 暗号は、図 2 に示すように、① 複数の登録者が確認者の公開鍵を用いてデータを暗号化してサーバに送り、② サーバが秘密計算を行って暗号化計算結果を確認者に送り、③ 確認者が自身の秘密鍵で復号して計算結果を取得する、という使い方をする。

\*4 本方式は処理時間に課題があり、現時点では、大規模なデータ分析や複雑な処理に対して、実用レベルに達しているとは言い難い。

### 3.2 Paillier 暗号の適用上の課題

前述の通り Paillier 暗号は、加法に関して準同型の性質を持つ。それ故、Paillier 暗号の適用により、個々のデータが End-to-End で暗号化されていても、集計受付センタでは世帯合算値を計算することができるようになる。

しかし、Paillier 暗号を直接、我々が提案するモデルに適用させようとした場合、次の課題が生じる。

通常 Paillier 暗号では、登録者が各データを確認者の公開鍵で暗号化する。そこで、図 3 の様に、各実務主体（登録者）がある医療機関（確認者）の公開鍵  $pk_V$  を使って各データを暗号化し、集計受付センタに登録するケースを考察してみる。この場合、集計受付センタでは秘密計算により暗号化状態のまま世帯合算値を計算し、医療機関（確認者）では自身の秘密鍵  $sk_V$  を使ってその暗号化計算結果を復号することができる。

しかし、この適用方法では、暗号化計算結果を復号することができるのは、秘密鍵  $sk_V$  を有する医療機関（確認者）のみであり、他のサービス事業者（確認者）は、計算結果を取得できなくなる。勿論、全サービス事業者（確認者）が同一の秘密鍵  $sk_V$  を予め共有すれば、全サービス事業者（確認者）は暗号化計算結果を復号できるようになるが、その場合、一か所からでも秘密鍵  $sk_V$  が漏洩した際、システム全体のセキュリティを保てなくなる。これらは【要件 3】に反する。

また、図 4 の様に、集計受付センタの公開鍵  $pk_S$  を使って各実務主体（登録者）がデータを暗号化する方法も考えられる。この場合、集計受付センタが計算した暗号化計算結果は、一旦、集計受付センタで復号し、その復号した計算結果を各確認者に SSL 通信などを使って送付することにより、システム共通の秘密鍵を全確認者に予め共有させることなく、複数の確認者に計算結果を利用させることが可能になる。

しかし、この適用方法では、暗号化計算結果および個々の暗号化データは、集計受付センタの公開鍵  $pk_S$  で暗号化されているので、集計受付センタは、自身の秘密鍵  $sk_S$  にて暗号化計算結果および個々の暗号化データを復号できてしまう。これは【要件 2】に反する。

以上より、直接 Paillier 暗号を提案モデルに適用するには、課題が存在することが分かった。そこで、我々は Paillier 暗号のプロトコルを改良し、全てのセキュリティ要件を満たす秘密計算方式を設計した。次章にて、提案方式を説明する。

## 4. 多対多の暗復号化可能な秘密計算方式の提案

### 4.1 提案方式のラフスケッチ

そもそも Paillier 暗号は、図 2 に示すように、複数の登録者がデータを暗号化することができるが、その暗号化デー

図 3 Paillier 暗号の適用上の課題（適用モデル 1）

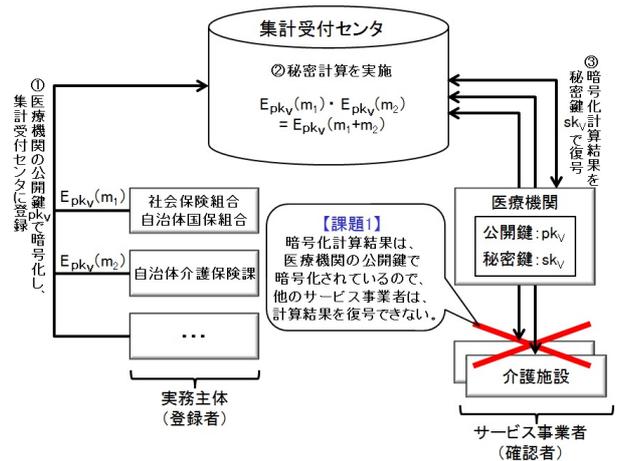
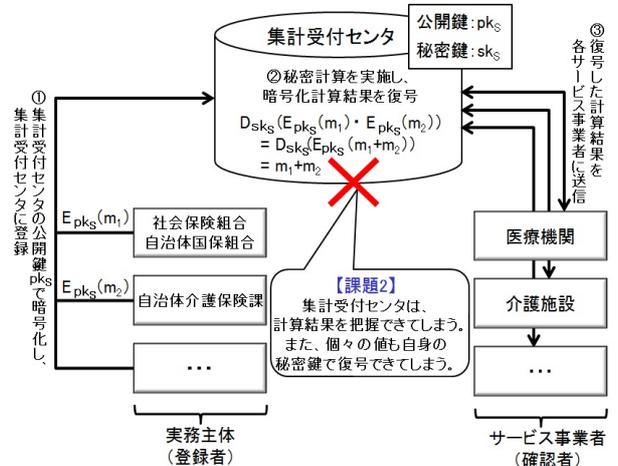


図 4 Paillier 暗号の適用上の課題（適用モデル 2）



データを復号できるのは、対応する秘密鍵を有している確認者のみである。つまり、Paillier 暗号は、多対 1 の暗復号可能な方式なのである。

一方、提案モデルでは、登録者だけではなく、確認者も複数存在する。つまり、提案モデルへの適用には、多対多の暗復号可能な方式が必要なのである。これが Paillier 暗号の適用に対して、課題が生じた原因である。そこで我々は Paillier 暗号を多対多の暗復号ができるように改良した。まずは、その改良ポイントを説明する（図 5 参照）。

改良ポイントは大きくわけて 2 つある。

一つ目のポイントは、「集計受付センタ」を「集計センタ」と「受付センタ」の 2 つに分けたことである。そして暗号化データの集計処理と Paillier 暗号の秘密鍵管理を各々のセンタに分担させた。暗号化データの内容を見る為には、対象となる暗号化データと復号に用いる秘密鍵の両方が必要である。そこで、暗号化データの管理と秘密鍵の管理を各センタに分けることにより、単独センタでの不正閲覧を防止した（【要件 2】対応）。

二つ目のポイントは、Paillier 暗号と ElGamal 暗号 [4] を組み合わせることである。Paillier 暗号での秘密計算結

図 5 提案方式のポイント

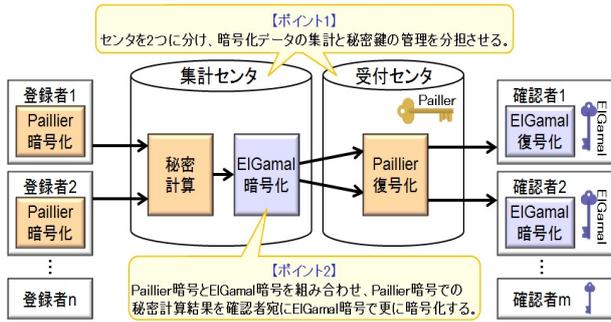
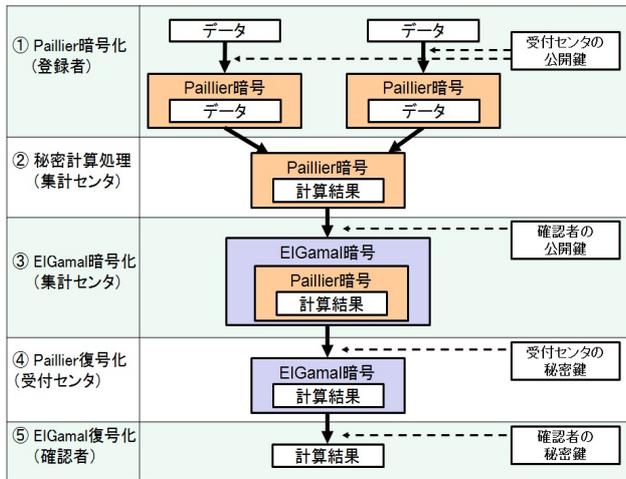


図 6 提案方式でのデータの流れ (イメージ)



果を確認者宛に ElGamal 暗号を使って更に暗号化させることで多対多の暗復号を可能にした(【要件 3】対応)。

より具体的には、提案方式では、Paillier 暗号の鍵ペアは、受付センタで生成する。また、各確認者は夫々 ElGamal 暗号の鍵ペアを生成する。

登録者は受付センタの公開鍵で Paillier 暗号を用いてデータを暗号化し、集計センタに登録する(図 6①)。

集計センタでは、必要に応じて秘密計算処理を行う。このとき集計センタでは秘密鍵を保持していないので、各暗号化データや暗号化計算結果を復号することはできない(図 6②)。

また、集計センタでは計算結果を暗号化状態のまま、確認者の公開鍵で ElGamal 暗号を用いて更に暗号化する(図 6③)。

受付センタでは、二重に暗号化された計算結果の内、自身の秘密鍵で Paillier 暗号文部分を復号し、それを確認者に送信する(図 6④)。このとき計算結果は ElGamal 暗号で暗号化されている状態にあるので、受付センタでも計算結果を把握することはできない。

そして確認者は、自身の秘密鍵で受付センタから送られてきた暗号化計算結果を復号する(図 6⑤)。

## 4.2 提案方式の詳細

最後に提案方式の詳細を説明する(図 7, 図 8 参照)。

尚、本論文で用いる関数を以下の様に表記する。

- 提案方式の暗号化関数:  $E_{pk}()$ ,
- 提案方式の復号関数:  $D_{sk}()$ ,
- Paillier 暗号化関数:  $E_{pk}^P()$ ,
- Paillier 復号関数:  $D_{sk}^P()$ ,
- ElGamal 暗号化関数:  $E_{pk}^E()$ ,
- ElGamal 復号関数:  $D_{sk}^E()$ 。

本方式は、鍵ペア生成フェーズ、データ暗号化フェーズ、秘密計算処理フェーズの 3 フェーズに分かれる。以下、フェーズ毎に詳細を説明する。

### 4.2.1 鍵ペア生成フェーズ

受付センタの鍵ペア生成

受付センタは大きな素数  $p$  および  $q$  を選び、 $n = p \cdot q$  とする。また、 $k \in Z_n^*$  を任意に選び、 $g = 1 + k \cdot n \bmod n^2$  とする。さらに位数が  $\lambda = \text{lcm}(p-1, q-1)$  なる  $G \in Z_n^*$  を任意に選ぶ。そして、 $pk_S = (n, g, G)$  を受付センタの公開鍵として各ステークホルダに公開する。

このとき受付センタでは、パラメータ  $b$  を  $\frac{n}{2}$  より小さい自然数から選び、各ステークホルダに公開しておく。尚、この公開パラメータ  $b$  は演算を行う項数の最大値を表す。つまり、本システムでは、最大  $b$  個までの加法または減法の演算ができる。

そして、受付センタでは、 $sk_S = (p, q)$  を秘密鍵として安全に管理する。

各確認者の鍵ペア生成

確認者  $V_i$  は、 $x_i \in Z_n^*$  を任意に選び、 $sk_{V_i} = x_i$  を自身の秘密鍵として安全に管理する。また、 $y_i = G^{x_i} \bmod n$  を計算し、 $pk_{V_i} = y_i$  を確認者  $V_i$  の公開鍵として受付センタに登録する。

### 4.2.2 データ暗号化フェーズ

登録者は、暗号化対象のデータとして平文  $m \in Z_{\frac{n}{2b}-1}$  を選び、受付センタの公開鍵  $pk_S$  で平文  $m$  を Paillier 暗号を用いて暗号化する。

$$c = E_{pk_S}(m) = E_{pk_S}^P(m) = g^m \cdot r^n \bmod n^2.$$

尚、 $r \in Z_n^*$  を乱数とする。

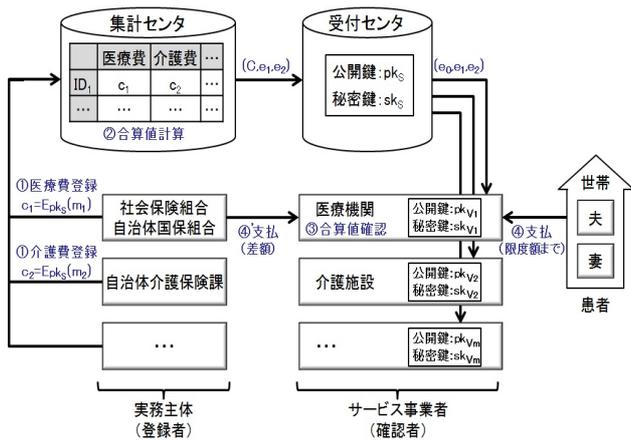
そして登録者は、暗号化データ  $c$  が何に対するデータであるかの属性情報(例えば“ID<sub>1</sub>”の“医療費”のデータであることを示す情報)を添えて、暗号化データ  $c$  を集計センタに送信する。

集計センタでは、指定された属性情報に従い、暗号化データ  $c$  を DB に登録する。

### 4.2.3 秘密計算処理フェーズ

確認者  $V_i$  は、演算範囲(例えば“ID<sub>1</sub>”の“医療費”と“介護費”の“和”を知りたい旨を示す情報)を指定して、受付センタに秘密計算依頼をする。

図 7 提案方式の概要



秘密計算依頼を受けた受付センタは、確認者  $V_i$  が本システムを利用できる確認者からのアクセスであるかを確認し、正当な確認者からのアクセスであれば、予め登録されている確認者  $V_i$  の公開鍵  $pk_{V_i}$  を取り出し、確認者  $V_i$  から受け取った演算範囲情報と共に集計センタに転送する。

集計センタでは、指定されている演算範囲を基に該当する暗号化データを選択する。ここでは、 $ID_1$  の医療費に対する暗号化データを“ $c_1$ ”とし、 $ID_1$  の介護費に対する暗号化データを“ $c_2$ ”として説明する。

まず、集計センタは、要求されている演算が“和”であるか“差”であるかを判断し、“和”であれば

$$c' = c_1 \cdot c_2 \text{ mod } n^2$$

を計算し、“差”であれば

$$c' = \frac{c_1}{c_2} \text{ mod } n^2$$

を計算する。

また、集計センタは  $s \in Z_n^*$  を任意に選び、

$$s' \cdot s = 1 \text{ mod } n$$

なる  $s'$  を計算する。

そして集計センタでは、

$$C = c'^s \text{ mod } n^2$$

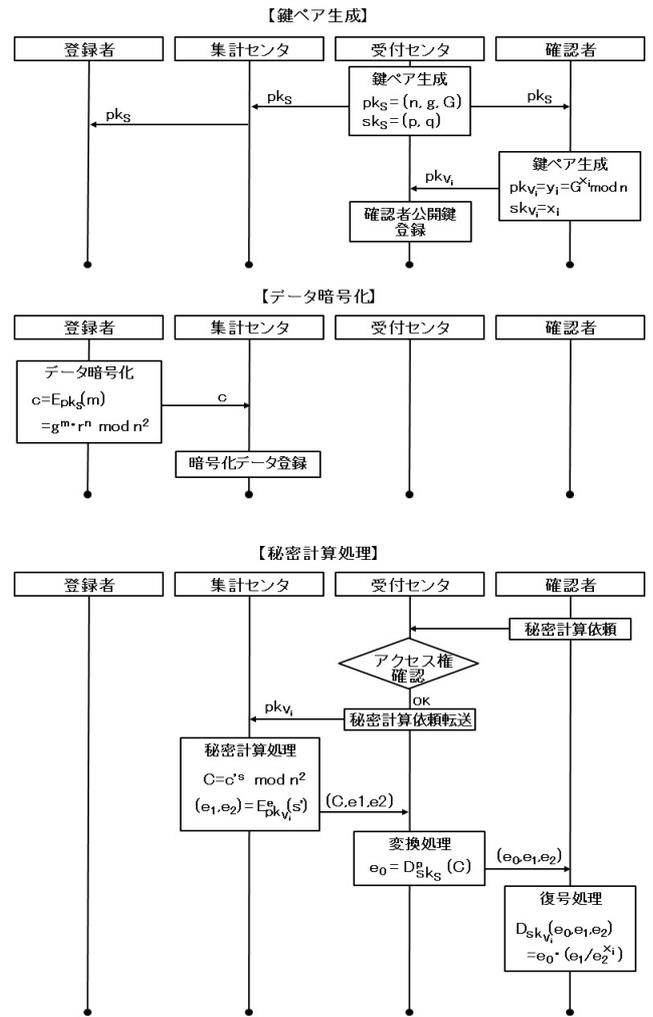
を計算し、さらに、 $s'$  を ElGamal 暗号を使って要求元の確認者宛に暗号化する。

$$\begin{aligned} E_{pk_{V_i}}^e(s') &= (e_1, e_2), \\ e_1 &= s' \cdot y_i^{r'} \text{ mod } n \quad (\forall r' \in Z^*), \\ e_2 &= G^{r'} \text{ mod } n. \end{aligned}$$

そして集計センタでは  $(C, e_1, e_2)$  を暗号化計算結果として受付センタに送る。

受付センタでは、集計センタから送られていた暗号化

図 8 提案方式のシーケンス



計算結果の内、 $C$  を自身の秘密鍵  $sk_S = (p, q)$  を用いて Paillier 暗号の復号処理を行う。

$$e_0 = D_{sk_S}^p(C) = \frac{L(C^\lambda \text{ mod } n^2)}{L(g^\lambda \text{ mod } n^2)} \text{ mod } n.$$

尚、 $\lambda = \text{lcm}(p-1, q-1)$  であり、 $L(x) = \frac{x-1}{n} \text{ mod } n^2$  である。

そして受付センタは要求元の確認者  $V_i$  に  $(e_0, e_1, e_2)$  を暗号化計算結果として送信する。

確認者  $V_i$  は、受付センタから送られていた暗号化計算結果  $(e_0, e_1, e_2)$  を自身の秘密鍵  $sk_{V_i} = x_i$  を用いて以下の復号処理を行う。

$$\begin{aligned} m' &= D_{sk_{V_i}}(e_0, e_1, e_2) \\ &= e_0 \cdot D_{sk_{V_i}}^e(e_1, e_2) \\ &= e_0 \cdot \frac{e_1}{e_2^{x_i}} \text{ mod } n. \end{aligned}$$

ここで復号された  $m'$  に対して、 $m' < \frac{n}{2}$  であれば、 $m' = m'$  とし、 $m' \geq \frac{n}{2}$  であれば、 $m' = m' - n$  とする。

このとき、 $m'$  が求める計算結果であることは以下より

わかる .

各暗号化データ  $c_1$  および  $c_2$  を ,

$$\begin{aligned} c_1 &= g^{m_1} \cdot r_1^n = g^{m_1} \cdot r_1^n \bmod n^2, \\ c_2 &= g^{m_2} \cdot r_2^n = g^{m_2} \cdot r_2^n \bmod n^2 \end{aligned}$$

としたとき ,

$$c' = c_1 \cdot c_2 = g^{(m_1+m_2)} \cdot (r_1 \cdot r_2)^n \bmod n^2$$

であり ,

$$C = c'^s = g^{s \cdot (m_1+m_2)} \cdot (r_1 \cdot r_2)^{s \cdot n} \bmod n^2$$

である . そして ,  $C$  を Paillier 復号関数に入力すると  $g$  の指数部分の値を出力するので

$$e_0 = D_{sk_S}^p(C) = s \cdot (m_1 + m_2) \bmod n$$

が得られる . 一方 ,  $(e_1, e_2)$  は ,  $s'$  を ElGamal 暗号で暗号化した値なので , 復号すると ,

$$D_{sk_{V_i}}^e(e_1, e_2) = \frac{e_1}{e_2^{x_i}} = \frac{s' \cdot y_i^{r'}}{G^{r' \cdot x_i}} = \frac{s' \cdot G^{x_i \cdot r'}}{G^{r' \cdot x_i}} = s' \bmod n$$

が得られる . 故に ,

$$\begin{aligned} m' &= D_{sk_{V_i}}(e_0, e_1, e_2) \\ &= e_0 \cdot D_{sk_{V_i}}^e(e_1, e_2) \\ &= s \cdot (m_1 + m_2) \cdot s' \\ &= (m_1 + m_2) \bmod n \end{aligned}$$

となる . ここで  $m_1, m_2 \in Z_{\frac{n}{2b}-1}$  であるので  $m_1 + m_2 < \frac{n}{2}$  であり , それ故  $m'$  は ,  $m' = m_1 + m_2$  であることがわかる .

## 5. まとめ

本論文では , 高額医療・高額介護合算療養費制度等における「自己負担額の世帯合算および現物給付サービス」の仕組みを電子的に実現する方法について , まず , モデル化を行い , そのモデルに従ってセキュリティ要件を定義した .

また , このセキュリティ要件と照らし合わせることで , 既存の秘密計算技術 ( Paillier 暗号 ) を適用する際の課題を整理した . そして , Paillier 暗号は多対 1 の暗復号方式であることが課題が生じた原因であり , 本モデルへの適用には , 多対多の暗復号可能な秘密計算技術が必要であることがわかった .

そこで , 我々は , Paillier 暗号と ElGamal 暗号とを組み合わせることにより課題を解決し , 多対多の暗復号可能な秘密計算プロトコルを提案した . 提案方式と Paillier 暗号との比較を表 1 に示す .

## 参考文献

[1] Pascal Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EURO-CRYPT'99, vol. 1592 of Lecture Notes in Computer Science, pp.223-238, 2009

表 1 提案方式と一般的な Paillier 暗号との比較

	要件 1	要件 2	要件 3
提案方式			
Paillier (適用モデル 1)			×
Paillier (適用モデル 2)		×	

( : 要件を満たす , × : 要件を満たさない)

- [2] R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” Comm. ACM, 21, 21, pp.120-126, 1978.
- [3] Craig Gentry, “Fully homomorphic encryption using ideal lattices,” STOC2009, pp.169-178, 2009
- [4] T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” IEEE Transactions on Information Theory, Vol.31, No.4, pp.469-472, 1985
- [5] 厚生労働省, “総合合算制度の導入,” <http://www.mhlw.go.jp/stf/shingi/2r985200000297nt-att/2r98520000029af4.pdf>, [Accessed July 2016]
- [6] 辻井重男, 山口浩, 只木幸太郎, 角尾幸保, “Paillier 暗号と RSA 暗号の連携による暗号化状態処理の一方式 電子行政・医療介護ネットワークにおける個人情報の保護と利用の両立を目指して,” SCIS2012, 3A1-3, 2012
- [7] “大阪市の戸籍不正アクセスは 62 人 , 上司含め 188 処分外部流出はなし,” <http://www.sankei.com/west/news/150312/wst1503120040-n1.html>, [Accessed July 2016]
- [8] “報告:住民基本台帳情報等の目的外利用について,” [www.city.kobe.lg.jp/information/public/hogo/img/400300.pdf](http://www.city.kobe.lg.jp/information/public/hogo/img/400300.pdf), [Accessed July 2016]
- [9] “Credit Card Processor Says Some Data Was Stolen,” New York Times, January 20, 2009, [http://www.nytimes.com/2009/01/21/technology/21breach.html?\\_r=3&ref=technology&](http://www.nytimes.com/2009/01/21/technology/21breach.html?_r=3&ref=technology&), [Accessed July 2016]