Vol.2013-CSEC-62 No.15
Vol.2013-SPT-6 No.15
2013/7/18

非対称秘密分散法を用いたアプリケーションの検討

高橋 慧[1,a)]　岩村 恵市[1]

概要：CSS2012 で我々が提案を行った秘密分散法の大きな特徴は，特定のサーバの記憶容量を非常に小さくすることができるということである．これは，この様な記憶容量の削減を行うサーバを携帯端末や記憶容量をほとんど持たない小さな装置とすることができ，従来法の様に各サーバの記憶容量を均等に削減する方式に対して新たな応用を生み出す可能性がある．そこで，CSS2012 方式を SCIS2013 において提案されたスマートグリッドに適用し，顧客のプライバシー保護と需要家の電力消費に関する統計計算を同時に実現する応用を構成し，今までにないメリットが実現できることを示す．その他にも，今まで考えられなかった携帯端末や IC カードをデータの分散を行うサーバとする新しい応用を検討する．

1. はじめに

近年，クラウドコンピューティングの普及に伴い，クラウド上に蓄積された膨大な量の情報を分析して新たな価値創造につなげる，ビックデータの利用活用への期待が高まっている．クラウドコンピューティングとはユーザの持つデータをクラウドと呼ばれるネットワーク上の複数のサーバにより構成される仮想の大容量ストレージに分散・保管し，そのデータをネットワーク経由でユーザが必要に応じてアクセスすることを可能にする技術である [1][2]．一方で，これらのデータには個人情報などの各個人に関するプライベート情報が含まれており，これらの機密情報の流出が大きな社会問題となっている．

現在，この様なクラウドシステムを構成する際に，秘密分散法を適用し，これらのプライバシ情報の漏洩を防止する試みがなされている．秘密分散法は次のような特徴を持つ．

(1) 1 つのデータを複数のサーバに分散し，これらのデータのうちいくつかが破損しても元のデータを復元することができる．
(2) 各サーバに分散されている分散情報をある閾値以上の個数集めない限り元の秘密情報を復元することができない．

この様な特徴を持つ秘密分散法として最も有名なものが Shamir により提案された (k,n) 閾値秘密分散法 [3] である．この方式では n 台のサーバに $k-1$ 次の多項式を用いて生成した分散情報をそれぞれ保存する．そしてこのうち k 台のサーバの持つ分散情報を集めることで元の秘密情報を完全に復元でき，$k-1$ 台以下のサーバから分散情報を集めても元の秘密情報に関する情報を一切得ることができない．また，この方式では各サーバが複数の秘密情報に関する分散情報を持つ場合には，それぞれの分散情報同士で演算を行い，演算結果を用いて秘密情報を復元することで秘密情報を秘匿したまま秘密情報同士の演算を行うことができる準同型性を持つ．しかし，この方式において生成される分散情報のデータサイズは元の秘密情報のデータサイズよりも小さくすることができないため，ビックデータのように膨大な量のデータを取り扱うシステムでは分散情報を保管する全てのサーバが非常に多くの記憶容量を持つ必要があるため，システムの構成に非常に大きなコストが掛かってしまうという問題点がある．

この問題を解決する方法として Rmap 型秘密分散法 [4] が提案されている．この方式では各サーバの持つデータ量を前述の (k,n) 閾値秘密分散法に比べ $1/L$ 倍にすることができる．しかし，この方式の場合，各サーバに分散する分散情報のデータサイズを縮小すればするほど閾値である k 個未満の分散情報から秘密情報に関する段階的な漏洩が生じるため，安全性に問題が生じてしまう．また，この方式では前述の (k,n) 閾値秘密分散法のように準同型性を持たないため，分散情報同士で演算を行っても，演算結果を復元することができない．

これらの方式に対して，我々は CSS2012 において新しい秘密分散法の提案を行った [7](以降：非対称秘密分散法)．この方式では従来方式の様に分散情報のデータサイズ自体を縮小するというアプローチではなく，特定のサーバの持

[1] 東京理科大学
Tokyo University of Science,
Katsushika, Tokyo 125-8585, Japan
[a)] takahashi@sec.ee.kagu.tus.ac.jp

ⓒ 2013 Information Processing Society of Japan

つ分散情報の個数自体を削減するというアプローチでシステム全体で持つデータ量の削減を実現する．この方式を用いることで，削減を行ったサーバの持つデータ量を鍵情報のみとすることができる．

このように，非対称秘密分散法を利用してシステム構築することで，これまでの秘密分散法では実現が困難であった特定の機器についてほとんどデータ量を持つことなく膨大な量のデータを管理することが可能となる．これにより，端末の管理が容易となるため，これまで，ある程度事業者側のセキュリティ要項などに依存してしていたビックデータの利用法をユーザが直接制御することが可能となる．

本論文では前述の非対称秘密分散法を適用したアプリケーションの一例として，「スマートグリッド」について考える．「スマートグリッド」とは，次世代電力網として世界各国で導入が検討されているシステムであり，各需要家の電力情報をスマートグリッドと呼ばれる装置で記録し，MDMS(Meter Data management System) と呼ばれる装置に送信し，電力系統の制御や課金などに利用される．この場合，MDMS は単位時間ごとの各家庭の電力使用量を逐次把握することができるため，その過程の 1 日の生活習慣や家庭内の使用機器といったプライバシ情報が MDMS に対して漏洩することとなる．そのため山中らは SCIS2013 において秘密分散法を用いたスマートグリッドにおけるプライバシ保護方式を提案した [8]．この方式ではこれらのメーターデータを直接 MDMS に保存するのではなく，秘密分散法を用いて分散を行うことで，それぞれの MDMS からはメータデータを得られない形に変換し，需要家のプライバシを保護する．しかし，この場合には大きな記憶容量を持った MDMS を 2 台用意する必要があり，さらに 2 台の MDMS へデータを送信するための送信網を構築するなど比較的大きな規模でシステムの構成を変更する必要があるため，システム構成に大きな設備投資コストが掛かってしまう．そこで，この方式に対して非対称秘密分散法を適用することで，大きなシステム変更をすることなく，最低限の設備投資コストで需要家のプライバシ情報を保護することができる方式を提案する．

また，もうひとつの例として，ライフログビジネスについて考える．「ライフログ」とは，一般的に，ある消費者の行動記録をデジタル化し集積したものを意味する．これらの消費者の行動情報から統計データを得ることで事業者は個人の好みに応じたサービスを提供することができる．しかし，この様な行動情報についても前述のスマートグリッド同様各消費者のプライバシ情報を含む情報であり，外部への漏洩は防がれるべきである [9]．しかし，これらのライフログは膨大なデータ量となるため，消費者が通常携帯するモバイル端末や IC カードなどで全ての情報を管理することは困難である．そこで，ライフログに対して前述の非対称秘密分散法を適用し，外部への情報の漏洩を防ぎつつ，統計データの生成等を消費者が制御することができる方式を提案する．

本論文の構成を以下に示す．第 2 章において秘密分散法の従来方式について説明を行う．その後第 3 章では，我々が CSS2012 において提案した非対称秘密分散法について説明を行う．そして第 4 章では非対称秘密分散法を適用するアプリケーションの一つとしてスマートグリッドに適用する場合を示し，第 5 章ではもう一つの適用例としてライフログに適用した場合について説明を行う．

2. 従来方式

本章では，秘密分散法の基本的な手法である Shamir の (k,n) 閾値秘密分散法及び (k,L,n) ランプ型秘密分散法の紹介を行う．

なお，本論文全体を通じて秘密分散に関する計算は秘密情報を s，ユーザが秘密情報を分散するサーバの台数を n としたとき，$s < p$ かつ $n < p$ である素数 p による $(modp)$ 上で行うものとする．つまり本論文においてすべての秘密分散に関する計算は p 個の要素を持つ GF(p) 上で計算される．また，分散する秘密情報の個数を m とし，簡単のため全秘密情報と分散情報のサイズを同じとし，$|s|$ と表す．

2.1 (k,n) 閾値秘密分散法

次の二つの条件を満たす秘密分散法を，(k,n) 閾値秘密分散法と呼ぶ．

(1) k 個以上の任意の分散情報から，元の秘密情報 s を完全に復元することができる．
(2) $k-1$ 個以下の分散情報からは，秘密情報 s に関する情報は一切得ることができない．

Shamir の提案した多項式補間による方法では，以下の様にして (k,n) 閾値秘密分散法を実現する．

[分散]

(1) $s < p$ かつ $n < p$ である任意の素数 p を選ぶ．
(2) $GF(p)$ の元から，異なる n 個の $x_i (i = 1, \cdots, n)$ を選びだし，各サーバの識別子とする．
(3) $GF(p)$ の元から，$k-1$ 個の乱数 $a_l (l = 1, 2, \cdots, k-1)$ を選んで，以下の式を生成する．

$$f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \quad (1)$$

(4) 上記式 (1) の x に各サーバの識別子 x_i を代入して，n 個の分散情報 $f(x_i) = W_i (i = 1, 2, \cdots, n)$ を計算し，各サーバに x_i と生成した W_i を送信する．

[復元]

(1) 復元に用いる分散情報を n 個の分散情報 $W_i (i = 1, 2, \cdots, n)$ から k 個選択し $W_{if} (f = 1, 2, \cdots, k)$ とする．また，その分散情報に対応するサーバ識別子を x_{if}

とする．

(2) 分散式 $f(x)$ に $x = x_{if}$ 及び $f(x_j) = W_{if}$ を代入し，k 個の連立方程式を解いて，秘密情報 s を得る．s の復元の際には，Lagrange の補間公式を用いると便利である．

この (k,n) 閾値秘密分散法を m 個の秘密情報に対して独立に行うことを考える．この場合，システム全体で必要な記憶容量は $m \times n \times |s|$ となる．

この方式では閾値 k 台以上のサーバの持つ分散情報を集めることで，元の秘密情報を完全に復元することができ，各分散情報についても情報量的安全性を持つことが知られている．また，この方式は準同型性を持つため，複数の秘密情報に関する分散情報同士を演算することで，任意の演算結果を得ることができる．しかし，この方式の場合，分散情報のデータサイズを元の秘密情報のデータサイズよりも小さくすることができないため，非常に容量効率が悪い．

2.2 Ramp 型秘密分散法

ランプ型秘密分散法は，以下の条件を満たす．

(1) 任意の k 個以上の分散情報から、元の秘密情報 s を完全に復元することができる．

(2) 任意の $k-t$ 個 $(1 \leq t \leq \text{L-1})$ の分散情報からは，段階的に秘密情報 s の情報が得られる．

(3) $k-L$ 個以下の分散情報からは，秘密情報 s に関する情報は一切得ることができない．

多項式補間を利用した (k,n) 閾値秘密分散法を変更することで，以下の様にランプ型秘密分散法を実現できる．ここで秘密情報を $s = (s_0, s_1, \cdots, s_{L-1})$ とし，分散式を以下の様に定めて，分散情報 W_i を計算する．

$$W_i = s_0 + s_1 x_i + s_2 x_i^2 + \cdots + s_{L-1} x_i^{L-1} + a_L x_i^L + \cdots + a_{k-1} x_i^{k-1} \quad (2)$$

復号の際には，(k,n) 閾値秘密分散法と同様の手順で連立方程式を解き $s_0, s_1, \cdots, s_{L-1}$ を求める．

この方式を用いた場合，m 個の秘密情報を分散した場合でもシステム全体で必要となる記憶容量は $(m \times n \times |s|)/L$ となるため，(k,n) 閾値秘密分散法を独立に繰り返した場合に比べ，システム全体の記憶容量を $1/L$ に削減できる．しかし，この方式は復元過程において $k - L + 1$ 個以上の分散情報が集まると段階的に秘密情報が漏えいすることが知られている [10]．また，この方式は前述の (k,n) 閾値秘密分散法とは異なり，準同型性を持たないため，分散情報の状態で秘密情報同士を演算することが不可能である．これよりこの方式を統計データの生成が必要となるシステムに適用することは困難であると考えられる．

3. 非対称秘密分散法

本章では我々が CSS2012 において提案を行った非対称秘密分散法について説明を行う．2 章において説明を行った (k,n) 閾値秘密分散法では分散情報それぞれのデータサイズを元の秘密情報のものよりも小さくできないため，容量効率が悪いという問題点があった．また，この問題を解決する方式として提案された (k,L,n) ランプ型秘密分散法の場合には，分散情報のデータサイズを (k,n) 閾値秘密分散法に比べ $1/L$ にすることができたが，閾値である k 個未満の分散情報から秘密情報に関する情報が段階的に漏洩してしまうという問題点があった．そこで，我々は従来方式のように分散情報自体のデータサイズを削減するのではなく，サーバの持つ分散情報の個数を削減するという新しいアプローチで，システム全体で持つべきデータ量の削減を実現した．

3.1 概要

本方式では図 1 に示すように，n 台のサーバから l 台を選択し，鍵サーバとする．これらの鍵サーバは分散情報を持たず，擬似乱数を生成するための鍵情報のみを持つため，分散情報の個数が削減される．鍵サーバはユーザの要求に応じて擬似乱数を生成し，ユーザはその疑似乱数を分散情報として分散式を決定する．そして，この際決定された分散式を用いて残りのサーバの持つ分散情報の算出を行う．ここで，この様な鍵サーバ以外の全ての秘密情報に関する分散情報を保管するサーバをデータサーバと呼ぶ．また，データを分散する各ユーザにはユーザ識別のため $ID[y](y = 1, \cdots, r)$ が割り当てられており，それぞれのユーザが持つ m 個の秘密情報 $s_{1j} \cdots s_{mj}(j = 1 \cdots r)$ にもそれぞれデータ識別のため $dID[s_{ij}](i = 1, \cdots, m)$ が割り振られているものとする．

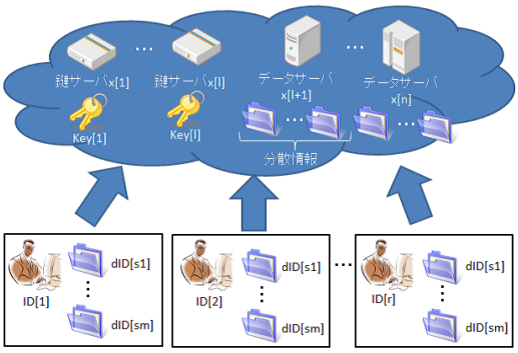

図 1 提案方式におけるシステム構成図
Fig. 1 Processing diagram of proposed method.

3.2 構成

まず，それぞれの秘密情報 $s_{ij}(i = 1, \cdots, m, j = 1, \cdots, m)$

について以下の分散式 $f(x)$ を生成する．ここで，提案方式においても全ての計算は GF(p) 上で行うものとする．

$$f(x)=s_{ij}+a_{i1}x+a_{i2}x^2+\cdots+a_{ik-1}x^{k-1} \quad (3)$$

各サーバには上記の分散式 $f(x)$ にそれぞれのサーバ識別子 x_j を代入した時に得られる値 $f(x_j)=W_{ij}$ を分散情報 W_{ij} として送信する．また，それぞれの秘密情報に割り振られているデータ識別子 $dID[s_{ij}]$ は秘密情報のデータサイズよりも小さいものとし，これらの $dID[s_{ij}]$ 及び秘密情報 s_{ij} の間には以下の関係があるとする．ただし，$H(A)$ は A という情報に関するエントロピーを表し，$H(A|B)$ は B という情報を知った時の A に関するエントロピーを表す．

$$H(s_{ij}|dID[s_{ij}])=H(s_{ij}) \quad (4)$$

本方式ではユーザが鍵情報のみを持つ鍵サーバにそれぞれのユーザ識別のために割り振られたユーザ識別子 $ID[y](y=1,\cdots,r)$ を送信し，それを受け取った鍵サーバが自身の持つ鍵 key_j と受け取った $ID[y]$ を用いて $Eid(y,j)=Enc(ID[y],key_j)(j=1\cdots l)$ を生成してユーザに送信する．ここで $Enc(a,b)$ は a を b という鍵を用いて暗号化する処理を表すとする．ユーザがこれを用いて自身のデータ識別子 $dID[s_{ij}]$ を暗号化し暗号化結果
$q_{ij}=Enc(dID[s_{ij}],Eid(y,j))$
を m 個の秘密情報全てについて生成したのち，これらが鍵サーバの分散情報に対応するように $W_{1j}=q_{1j},W_{2j}=q_{2j},\cdots,W_{mj}=q_{mj}$ としてそれぞれの秘密情報 $s_i(i=1\cdots m)$ に関する分散式 (3) 中の係数 $a_{i1},\cdots,a_{ik-1}$ を定める．以上を一般的に書くと提案方式の構成は以下のようになる．

ここで，分散情報を削減する鍵サーバの台数はクラウドシステム構成時に決定しており，l 台 $(2\le l\le k)$ とする．また，それぞれの秘密情報における分散式中の各係数を k 次のベクトルを用いて $A(i)=[s_{ij},a_{i1},\cdots,a_{ik-1}]^T$ と表す．

[分散]

(1) ユーザは自身の $ID[y](y=1,\cdots,r)$ を鍵サーバ $x_1,\cdots,x_l$ に送信する．

(2) $ID[y]$ を受け取った鍵サーバは自身の持つ暗号装置と鍵 key_j を利用して $Eid(y,j)=Enc(ID[y],key_j)(j=1,\cdots,l)$ を生成し，ユーザに送信する．

(3) これを受け取ったユーザは自身の秘密情報に関するデータ識別子 $dID[s_{ij}](i=1\cdots m)$ を用いて疑似乱数
$q_{ij}=Enc(dID[s_{ij}],Eid(y,j))$
を生成する．

(4) ユーザはまず前述の k 次の分散式の係数ベクトル $A(i)=[s_{ij},a_{i1},\cdots,a_{ik-1}]^T$ における $k-1-l$ 次の部分ベクトル $A'_{k-1-l}(i)=[a_{il+1},\cdots,a_{ik-1}]^T$ を真性乱数を用いて定める．その後，手順 (3) で生成した疑似乱数系列
$Q=[q_{1j},\cdots,q_{mj}]^T$ 及び鍵サーバの ID 系列

$$X'=\begin{bmatrix} x_1 & \cdots & x_1^{k-1} \\ \vdots & \ddots & \vdots \\ x_l & \cdots & x_l^{k-1} \end{bmatrix} \quad (5)$$

を用いて以下の式から分散式の係数ベクトル $A(i)$ における残りの部分ベクトル $A'_l(i)=[a_{i1},\cdots,a_{il}]^T$ を算出する．

$$A'_l(i)=X'^{-1}Q \quad (6)$$

これにより，ユーザは k 次の分散式の係数ベクトル $A(i)=[s_{ij},a_{i1},\cdots,a_{ik-1}]^T$ における $k-1$ 次の部分ベクトル $A(i)_{k-1}=[a_{i1},\cdots,a_{ik-1}]^T$ を決定することができる．

(5) また，ユーザはデータサーバ $x_{l+1},\cdots,x_n$ に関する分散情報 $W_{il+1},\cdots,W_{in}$ を手順 (4) で生成した係数行列を利用して (k,n) 閾値秘密分散法と同様の手順により算出する．

(6) ユーザはそれぞれのデータサーバに生成した分散情報 $W_{1j},\cdots,W_{mj}(j=l+1,\cdots,n)$ を送信する．

[復元]

(1) 秘密情報 s_i を復元するユーザは n 個のサーバ $x_1,\cdots,x_n$ から任意の k 個のサーバを選択し，選択したサーバに対して自身の $ID[y]$ 及び秘密情報 s_i のデータ識別子 $dID[s_{ij}]$ を送信する．

(2) 鍵サーバの中で，$(ID[y],dID[s_{ij}])$ を受け取ったサーバは自身の持つ鍵 key_j 及び暗号装置を利用して
$Eid(y,j)=Enc(ID[y],key_j)$
を生成し，疑似乱数
$q_{ij}=Enc(dID[s_{ij}],Eid(y,j))$
を生成してユーザに送信する．

(3) データサーバの中で，$(ID[y],dID[s_{ij}])$ を受け取ったサーバはこれらの ID 情報に対応する分散情報 W_{ij} をユーザに送信する．

(4) サーバにより生成された分散情報及び疑似乱数を受け取ったユーザは，これらを利用して (k,n) 閾値秘密分散法と同様の手段で，秘密情報 s_i を復元する．

これより本方式では各ユーザの $ID[y]$ 及び秘密情報 s_{ij} に割り振られた $dID[s_{ij}]$ を利用することで，鍵サーバが持つ情報は疑似乱数生成のための key_j のみでよく，この鍵情報を鍵サーバが安全に保管するという前提を置いた場合，すべてのユーザに共通で利用することができるため，ユーザの人数及び秘密情報の数に依存せず常にただ一つの鍵情報のみを持つだけでよいということになる．

4. スマートグリットへの秘密分散法の適用

本章では秘密分散法を適用したアプリケーションの一例

として SCIS2013 において東芝の山中らによって提案された秘密分散法を用いたスマートグリッドにおけるプライバシ保護方式 [8] について説明を行う．また，これらの方式の問題点を考察し，これらの問題点が我々の提案した非対称秘密分散法を適用することで解決することができるという事を示す．

4.1 スマートグリッド

以下の図 3 に米国 NIST が検討しているスマートグリッドの全体像を示す．

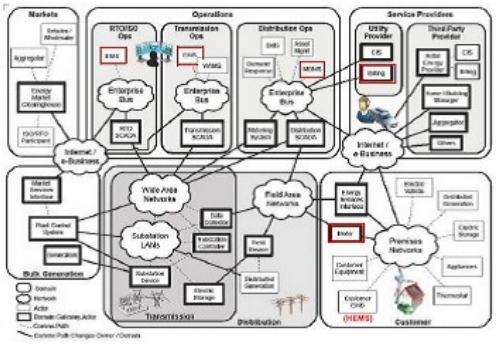

図 2 スマートグリッドコンセプト
Fig. 2 Concept of Smart Grid system.

スマートグリッドとは，発電や市場，送電，配電，サービス提供者，消費者といったドメインで構成される．そして，系統制御・需要管理のそれぞれに IT 技術を導入することにより，スマートグリッド化が実現される．

また，スマートグリッドには，消費者のスマートメータからの電力使用データを一元管理する MDMS(Meter Data Managemant System) が属しており，スマートグリッドでは各需要家はそれぞれの利用電力を MDMS へ送信する．これらの電力情報を受け取った MDMS は必要に応じて集計し，課金システムや発電側の電力周波数制御を行う EMS(Energy Management System) へ送信を行う．

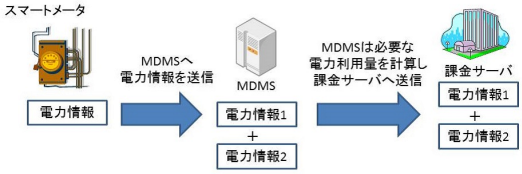

図 3 既存のスマートグリッドシステム
Fig. 3 Conventional system of Smart Grid.

4.2 秘密分散方式を用いるプライバシ保護

従来の電力システムでは検針員が 1 ヶ月単位で各家庭の電力利用料を電力メータから直接検針し，電力利用料の請求を行っていた．これに対して，スマートグリッドを用いたシステムの場合，これらの電力情報は単位時間ごとに MDMS へ送信を行うこととなるため，MDMS の保管する電力データから需要家の 1 日の生活習慣や家庭内の使用機器といったプライバシ情報が漏洩する可能性がある．これらの問題は 2010 年 3 月に EFF(Electronic Frontier Foundation) によって重大なプライバシ侵害を招くと表明されている．そのため，東芝の山中らは秘密分散法方式を用いてこれらの電力データを秘密情報として分散し，プライバシ情報の漏えいを防ぐ方式を提案した [8].

この方式では，以下の図 4 のようにスマートメータ，EMS，そして課金サーバは既存のものを流用する．そして，新たに電力利用情報の分割を行う主体として，Head End System 及び，電力情報の復元を行う主体として Application Adapter という主体を導入する．

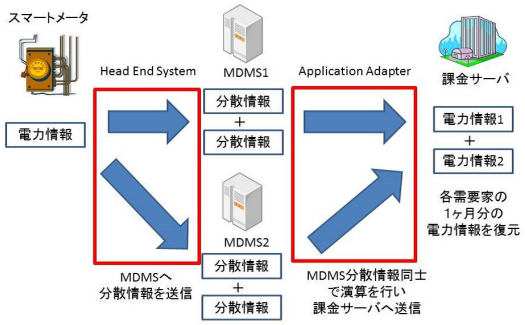

図 4 MDMS プライバシ保護システムの構成
Fig. 4 Configuration privacy protection of the MDMS.

この方式では，2.1 節で説明を行った (k,n) 閾値秘密分散法を用いて，電力情報の分散を行う．この場合システムとしては 2 台の MDMS を用意し，電力情報を (2,2) の秘密分散法を用いて分散を行う．これによりそれぞれの MDMS からは電力情報が漏洩することはない．

また，この方式において MDMS が課金サーバに対して料金徴収のためある需要家の 1 ヶ月分の電力利用量を送信する場合には，それぞれの MDMS において該当する需要家の電力情報から生成された分散情報を加算し，この結果を課金サーバに送信することで，課金サーバ側では 1 ヶ月分の合計利用電力情報は復元できるが，該当する需要家に関する 1 日ごとの電力利用情報に関しては一切の情報を得ることができない．

しかし，この方式では利用する秘密分散法として (k,n) 閾値秘密分散法を用いているため，MDMS が保存するデータ量に関して問題が発生する．なぜなら，(k,n) 閾値秘密分散法では生成される分散情報のデータサイズを分散を行

ⓒ 2013 Information Processing Society of Japan

う秘密情報のデータサイズよりも小さくすることができないためである．これよりこの方式では最低でもシステム全体で必要となる記憶容量は既存のシステムに比べ 2 倍となる．そのため，既存のシステムに対してデータ通信を行うシステムについて 2 台分用意する必要があり，非常に大きな設備投資コストが必要となることが考えられる．また，それぞれの分散情報を 2 台の MDMS に送信する際に攻撃者により通信路を盗聴された場合には二つの分散情報から電力情報を復元することが可能となるため，通信路についても暗号化を施す必要がある．

4.3 非対称秘密分散法のスマートグリッドシステムへの適用

前節で述べた山中らの方式ではシステムの構成に非常に大きな設備投資コストが必要となるという問題点があった．そこでこの様な問題を解決するため，前述の方式において適用する秘密分散法を (k,n) 閾値秘密分散法ではなく我々が提案を行った非対称秘密分散法を適用することを考える．これにより，既存のシステムとほぼ同じデータ量でありながら電力情報の秘匿性を両立することができるシステムを構成することができる．

具体的には従来方式における 2 台の MDMS のうち一台を非対称秘密分散法における鍵サーバと見なす場合を考える．この場合，鍵サーバとなった MDMS(MDMSk) には固有の鍵情報が割り振られ，課金サーバなどは各家庭の ID 情報を知っており，各需要家に設置されているスマートメータにはあらかじめ，MDMSk により ID 情報を暗号化されたデータ Eid が保管されているものとする．

実際に電力情報の分散を行う場合には，以下の図 5 のように各需要家は自身の持つ ID 情報の暗号化結果 Eid とタイムスタンプなどから生成されるデータ識別子 $dID[s_{ij}]$ を用いて疑似乱数 q_{ij} を生成する．その後スマートメータは電力情報を秘密情報として，前述の非対称秘密分散法と同様の手順で分散情報 W_{ij} を生成し，MDMS へ送信する．また，復元を行う場合には，MDMSk は対応する需要家の ID 情報を用いて擬似乱数を生成し，需要家へ送信する．また，通常の MDMS は自身の持つ分散情報を需要家へ送信し，これらを受け取った需要家は通常の秘密分散法と同様の手順により秘密情報である電力情報の復元を行う．

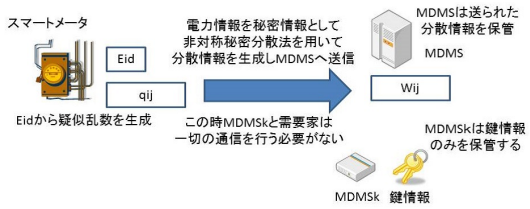

図 5 非対称秘密分散法を適用したスマートグリッドシステム
Fig. 5 Smart grid system applied Asymmetric secret sharing.

4.4 提案方式の特徴

前述のようにスマートグリッドを構成する際に非対称秘密分散法を用いることで，2 台の MDMS のうち，鍵サーバとなった MDMSk は鍵情報を持つのみでよく，もう一台の MDMS は基本システムと同様，前スマートメータから送られる情報を保存するだけでよい．また，この方式では各スマートメータから送信される情報は通常の MDMS に送信する分散情報のみであり，鍵サーバとなっている MDMSk に対しては一切の情報送信をする必要がないため，通信路を盗聴されたとしても，一切の情報漏えいが発生しない．このため，従来方式の様に，通信路に対しても，暗号化などの処理を行う必要がないといえる．このため，このシステムは既存のシステムに対して鍵を保存する鍵サーバを追加するのみでよく非常に小さな設備投資コストによって構成することができる．そして，課金サーバなどに対してある需要家の電力利用量の合計を送信する場合には，以下の図 6 全ての分散情報を持つ MDMS は該当する分散情報を加算し，鍵サーバとなった MDMSk は対応する需要家の ID 情報及びデータ識別子 dID から擬似乱数を生成し，これらの合計を取り，それぞれを課金サーバへ送信することで必要な集計データを課金サーバは復元することが可能となる．

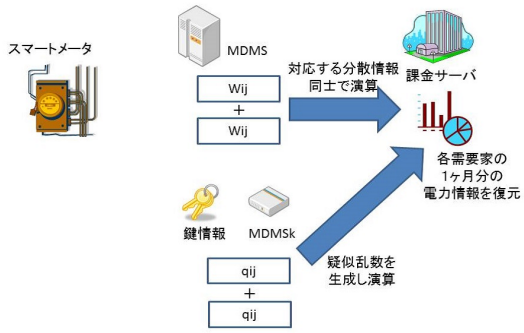

図 6 提案方式における電力利用量の生成
Fig. 6 Generation of electricity usage in the proposed method.

5. ライフログへの適用

5.1 ライフログ

ライフログとは一般的に，ある人間の行動記録をデジタル化し，集積したものを意味し，ウェブサイトの閲覧履歴，携帯端末による位置情報，IC 乗車券による乗車履歴などがこの行動記録にあたる．これらのライフログを利用することで，事業者側では，各消費者の好みに応じた様々なサービスを提供することが可能となり，非常に公共性の高いシステムであると考えられる．

5.2 ライフログにおけるプライバシ問題

前述のライフログにおいては前述のように事業者側で適

正に行動記録を利用されれば様々な利益を消費者は得ることができる．しかし，これらの行動履歴には，ある消費者が，何に興味を持ち，誰と一緒にいるか，何をしたかという情報を含むため，ひとたび，事業者側が扱い方を間違えた場合，個人のプライバシの漏えいに直結することとなる．事実，情報セキュリティ事故の約 70 %は紛失，誤送信などの過失に起因するものであり，さらに正当なデータ利用者が悪意を持って事故を起こした事例では，一度に 100 万件以上の個人情報の漏えいが生じている [9]．このような事例を考えると，これらのログを事業者側だけで管理することは避けるべきであり，統計データの生成についてもある程度消費者側で制御できることが望ましと考えられる．しかし，これらのライフログデータは非常に多くのデータで構成されており，消費者の持つモバイル端末や IC カード等の十分に大きな記憶容量を持たないデバイスでこれらのライフログデータを直接保管することは困難であると考えられる．

5.3 非対称秘密分散法の適用

本節ではライフログに対して非対称秘密分散法を適用したシステムについて提案を行う．このシステムではユーザ側の持つモバイル端末や IC カードを非対称秘密分散法における鍵サーバとみなすことで，以下の様な特徴を実現することができる．

(1) 消費者の持つ端末または事業者が管理するサーバのどちらかの情報が漏えいしただけでは，購入履歴や残高などに関する情報は一切漏えいしない．
(2) 事業者側は消費者の許可なく統計情報などの生成を行うことができない．
(3) 消費者が持つデータ量を鍵情報のみとすることができ，かつ分散時には計算量も暗号化に関するもののみとすることができるため，消費者の持つ端末にかかる負担が少ない．

5.3.1 ライフログデータの分散・復元

具体的なシステムは図 7 のように構成する．

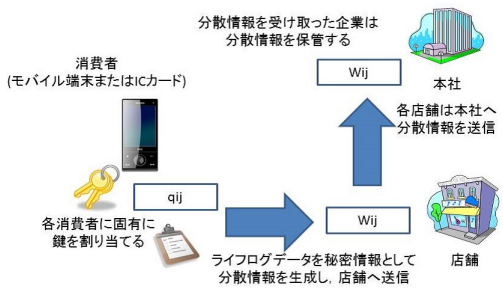

図 7 プライバシ保護を行ったライフログのシステム構成図
Fig. 7 Configuration of the privacy protected Life Log system.

このシステムにおいて各消費者の持つデバイスにはあらかじめ固有に鍵情報を割り振り，これらの鍵情報は信頼度の高い鍵管理サーバにより管理されるものとする．ここで，ある消費者 A がある事業者の店舗 B を利用した場合を考える．この場合ユーザは疑似乱数 q_{ij} を生成する．その後，ライフログとして記録したい行動情報を秘密情報 s_{ij} として，非対称秘密分散を実行し，分散情報 W_{ij} を生成し，これを受け取った店舗はこの分散情報のみを保管する．また，ユーザ側で復元を行う場合には，自身の持つ鍵情報を利用し，疑似乱数を生成後，事業者側に問い合わせを行い，事業者が持つ分散情報を受け取ることで自身の行動情報を復元することができる．

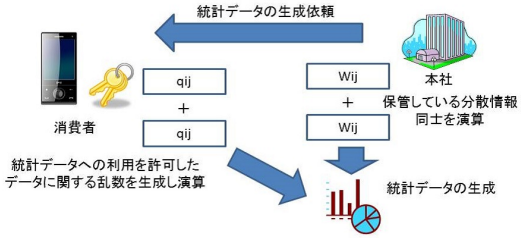

図 8 提案方式における統計データの生成
Fig. 8 Generation of statical data in the proposed method.

この方法により行動情報の分散を行うことで，各消費者は自身のモバイル端末や IC カードなどに乱数生成に利用する鍵情報を保存するのみで膨大な量のライフログデータを管理することが可能となる．また，事業者側で統計データを生成する場合には図 8 の様に事業者側で持つ分散情報のうち統計データ生成に必要な情報に関する分散情報に関して演算を行う．その後，消費者に対して事業者側からリクエストを送信し，統計データの生成を許可した消費者は自身の鍵情報を利用し，該当する行動情報に対応した疑似乱数を生成後，それらの乱数同士で演算を行い，演算結果を事業者へ送信する．これにより，消費者のプライバシを保護しながら，統計データの生成を行うことが可能であり，また，これらの統計データの生成に対して消費者側が同意しない場合，擬似乱数を生成しないことで，自身のライフログデータを統計データの生成に利用させないことが可能となるため，これによって，従来では困難であった消費者側で統計データの生成に関して制御を行うことが可能となる．

5.3.2 ライフログデータの漏洩防止効果

前述の様にライフログシステムに対して非対称秘密分散法を適用することで，図 9 の (a) の様に例え消費者の持つモバイル端末や IC カードなどが盗難され，内部情報を取得された場合でも攻撃者が得ることができる情報は擬似乱数生成に必要な鍵情報のみであり，この消費者に関するライフログ情報は一切得ることができない．

また，図 9 の (b) の様に分散情報を保管するサーバにお

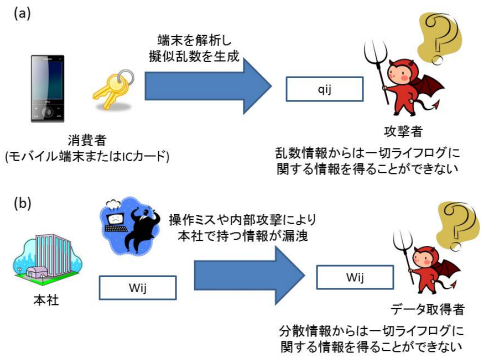

図 9 提案方式の情報漏洩耐性
Fig. 9 Prevention of information leakage of proposed method.

いて内部攻撃や操作ミス，誤送信などによって保管する分散情報が外部に漏洩したとしても，消費者に関するライフログを復元するためにはそれぞれの消費者が生成する擬似乱数が必要であるため，この様な脅威に対しても提案方式は耐性を持つこととなる．しかし，現実にはこの様なサーバや消費者の端末はパスワードやバイオメトリクスなどを用いて悪制御を行っていることが想定されるため，攻撃者は盗難端末に関する情報を利用することができない．

この他の特徴として，消費者が自身の持つ端末を紛失した場合，これらの端末に保管されている鍵データは鍵管理サーバにも同時に保管しておくことで，再度新たな端末に対して鍵を設定することが可能となり，データ自体を一切やり取りすることなく自身のライフログを復元することができる．

6. まとめ

本論文では，CSS2012 において我々が提案した非対称秘密分散法を適用したアプリケーションの一例としてスマートグリッド及びライフログを取り上げ，具体的なシステムについて説明を行った．

スマートグリッドシステムについては，非対称秘密分散法を適用することで，従来方式では既存システムの倍の台数必要で合った MDMS サーバの一台のサーバの持つデータ量を鍵情報のみとすることができるため，非常に小さな設備投資コストで需要家のプライバシ保護を実現するシステムを構築することができる．また，ライフログについては，非対称秘密分散法における鍵サーバをユーザの持つモバイル端末を用いて構成することで，従来では困難であった膨大な量の行動情報を消費者が管理することが可能となる．これにより，事業者が消費者の許可なく統計データの生成を行うことを防ぐことが可能となり，消費者の行動情報が外部に漏洩することを防止することが可能となる．

参考文献

[1] Peter Mell, Timothy Grance. NIST によるクラウドコンピューティングの定義. NIST(2011)
[2] M.Armbrust, A.Fox, R,Griffith, A.D.Joseph, R.Katz, A.Konwinski, G.Lee, D.Patterson, A.Rabkin, I.Stoica, M.Zaharia. A view of cloud computing. Communications of the ACM (2010)
[3] A. Shamir. How to share a secret. Communications of the ACM, 22, (11), pp.612-613 (1979)
[4] 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)
[5] G. R. Blakley. Security of ramp schemes. Crypto’84, pp.242-268 (1984)
[6] H. Krawczyk. Secret Sharing Made Short. Crypto’93, pp.136-146 (1994)
[7] 高橋慧，岩村惠市. クラウドコンピューティングに適した計算量的安全性を持つ秘密分散法. CSS2012 (2012)
[8] 山中晋爾，駒野雄一，伊藤聡. 秘密分散法式を用いたスマートグリッドにおけるプライバシ保護方式. SCIS2013 (2013)
[9] 石井夏生利. プライバシー・個人情報の「財産権論」～ライフログをめぐる問題状況を踏まえて. 総務省，情報通信政策研究所 (2012)
[10] 千田浩司，五十嵐大，濱田浩気，菊池亮，冨士仁，高橋克巳. マルチパーティ計算に適用可能な計算量的ショート秘密分散. SCIS2012 (2012)
[11] 千田浩司，五十嵐大，菊池亮，濱田浩気. 計算量的秘密分散およびランプ型秘密分散のマルチパーティ計算拡張. 情報処理学会研究報告書 (2012)
[12] Michael.ORabin. Efficient dispersal of information for security, load balancing, and fault tolerance, Journal of the Association for Computing Machinery, pp.335-348 (1989)
[13] 土井洋. プライバシ保護技術に関する最新動向. 電子情報通信学会誌. vol.91,No.9,pp792-797 (2008)

ⓒ 2013 Information Processing Society of Japan