4Y-2

秘匿計算を用いたWeb会計システム

松村 太一† 岡村 真吾‡

†奈良工業高等専門学校 専攻科 ‡奈良工業高等専門学校 情報工学科

1 はじめに

現在，ブロードバンドネットワークの普及やサーバ仮想化技術の進歩により，クラウドコンピューティングが広く普及している．しかし，クラウドコンピューティングのようにユーザの情報をサービス提供者のサーバ上に保存する場合，サービス提供者による情報の悪用やプライバシーの侵害などの可能性がある．この問題に対して秘匿計算が有効である．秘匿計算とは自分の持つ値を相手に知られることなく，その値を用いた計算を相手に行ってもらえる計算手法であり，この秘匿計算をクラウド等に応用することで，ユーザの持つ情報をサービス提供者に秘匿することが可能である．本稿では秘匿計算の応用例としてWeb 会計システムを取り上げ，サービス提供者に対して金額情報，担当者などの会計情報を秘匿した状態で会計処理が可能な Web 会計システムを提案する．

2 Web会計システム

会計システムとは，金銭や物品の出納について貨幣を単位として記録・計算・管理などの会計処理を行うシステムであり，これらの会計処理は会計ルール従って行われる．会計ルールでは会計情報の取り扱い，金額の計算方法などが規定されている．Web 会計システムはこれらをWeb上で行うシステムである．

一般的な Web 会計システム[1]ではクライアントとして Web ブラウザが用いられる．またサーバは会計情報を保存するデータベースサーバ，会計ルールに従って会計処理を行うアプリケーションサーバ，SSL 通信等を行うWebサーバで構成される．

Web-Based Accounting System with Secure Computation
† Taichi MATSUMURA ‡ Shing OKAMURA
† Nata National College of Technology, Factory of Advanced Engineering
† Nara National College of Technology, Information Engineering

3 提案システム

3.1 システム要件

システム要件として，ユーザが入力する情報をサーバに対して秘匿可能(科目及び日付については秘匿しない)であり，その上でクライアントは会計情報の入出力，入力した会計情報についての部分一致検索および完全一致検索を行うことができることとする．秘匿する情報を表 1 に示す．また金額情報を用いた会計処理(四則演算により計算可能な損益計算，減価償却計算，原価計算，収支計算，予算管理など)を行うことができることとする．

表 1 秘匿する情報

秘匿する相手	秘匿する情報
サーバ	金額, 担当者などの会計情報
第三者	全ての入力情報

3.2 秘匿計算

提案システムでは，金額情報に対して完全準同型暗号による秘匿計算プロトコルを用いる．完全準同型暗号は Gentry[2]により提案され．任意の関数を構成することが可能[3]であるため，完全準同型暗号を用いることで任意の関数について秘匿計算を行う事が可能である．完全準同型暗号は暗号化関数 $E(\ )$と任意の演算”・”に対して(1)式を満たす．

$$E(x)\cdot E(y)=E(x\cdot y) \quad (1)$$

3.3 検索可能暗号

提案システムでは，金額情報以外の情報に対して検索可能暗号を用いる．検索可能暗号は暗号化された状態でデータ検索が可能な暗号方式であり，提案システムでは全文検索可能暗号[4]とキーワード検索可能暗号[5]の 2 つの方式を用いる．全文検索可能暗号では暗号化されたデータに対してワード検索を行う方式であり，キーワード検索可能暗号は暗号化されたデータに任意のキーワードを設定し，そのキーワー

ドを検索する方式である．全文検索可能暗号においては平文及び検索ワード，キーワード検索可能暗号においては平文，設定したキーワード，検索キーワードが秘匿される．

3.4 構成

提案システムの構成を表 2 及び図 1 に示す．

表 2 提案システムの構成要素

構成要素	機能・役割
Web ブラウザ	会計情報の入力 会計処理の要求 Web サーバとの通信
Web サーバ	Web ブラウザとの SSL 通信等
アプリケーション サーバ	会計ルールに従った 会計処理
データベースサーバ	会計情報の保存・管理
秘匿計算サーバ	準同型暗号による 秘匿計算
検索サーバ	検索可能暗号による 検索

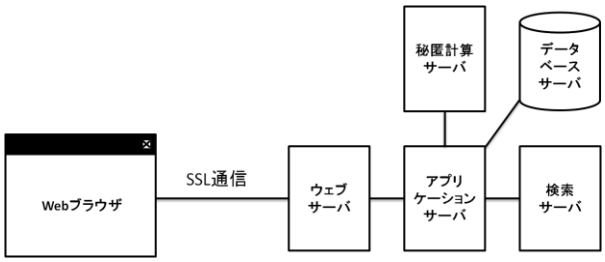

図 1 提案システムの構成

3.5 処理

入力：Web ブラウザは金額情報を準同型暗号，それ以外を全文検索可能暗号またはキーワード検索可能暗号により暗号化し Web サーバに送信する．Web サーバはこれらの会計情報をアプリケーションサーバ経由でデータベースサーバに格納する．

出力：Web ブラウザからの処理要求に対して，アプリケーションサーバが日付，科目などをもとに必要な情報をデータベースサーバから取り出し，会計処理を行う．この時金額情報は暗号化されているがそのまま計算を行う．処理結果を Web ブラウザに送信し，Web ブラウザは暗号化されている部分を復号する．準同型暗号の性質より，暗号化前の金額情報を用いた処理結果を得る．

検索：Web ブラウザは検索用の鍵と検索ワードまたは検索キーワードを検索サーバに送る事で完全一致検索及び部分一致検索が可能である．

4 評価

完全準同型暗号および検索可能暗号が安全であれば，サーバに対して入力情報は漏れず，入力情報をサーバに対して秘匿可能である．また全文検索可能暗号およびキーワード検索可能暗号による検索の計算量は検索対象のデータ数 n に対して $O(n)$であり，システムの検索計算量は $O(n)$に従う．

5 まとめ

提案システムでは，サーバに対して入力情報の秘匿した状態で会計処理が可能である．しかし，暗号文から平文の操作が可能という準同型暗号の性質から，サーバによる金額情報の改ざんの可能性があり，今後の課題である．

参考文献

[1] Stewart Mckie 著, 橋本ら訳, インターネット環境化のクライアント/サーバ会計, 白桃書房, 1999.
[2] Craig Gentry, A fully homomorphic encryption scheme, PhD thesis, Stanford University, 2009.
[3] Craig Gentry, Computing Arbitrary Functions of Encrypted Data, Communications of the ACM Volume 53 Issue 3, pp. 97-105, March 2010.
[4] Dawn Xiaodong Song, Practical Techniques for Searches on Encrypted Data, In Proceedings of IEEE Symposium on Security and Privacy, pp. 44-55, May 2000.
[5] Boneh D, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Public-key encryption with keyword search, In proceedings of Eurocrypt, LNCS 3027, Springer-Verlag, pp. 506-522, 2004.