（ 続紙 1 ）

| 京都大学 | 博士（情報学） | 氏名 | 川本　淳平 |
|---|---|---|---|
| 論文題目 | A Study on User's Privacy Protection against Query Analysis in Cloud Databases（クラウドデータベースにおける問合せ解析からの利用者情報保護に関する研究） | | |

（論文内容の要旨）

文書管理や内部統制に関連する法改正に伴い，企業や組織はこれまで以上に膨大な量のデータを管理する必要に迫られている．また，災害対策のために物理的に離れた位置にデータのバックアップを用意する必要性も指摘されている．しかし，大規模データの管理システムの運用には保守管理コストやシステム攻撃に対する防衛コストなどが発生し，各組織が個別に運用することが難しい場合も多い．こうした状況に対して，低コストで高い可用性を持つサービスとしての情報システム，いわゆるクラウドサービスが注目されている．クラウドサービスは便利である一方，利用者は自身のデータやサーバを完全に制御することができず，サービス提供者を完全には信用することが難しい．本研究では，こうしたサービス提供者を完全には信用できないという仮定の下でもクラウドサービスを利用できるように，クライアントベースでセキュリティを確保することを目的としている．本博士論文では，このクラウドサービスをサービスが扱うデータを中心に議論するため，サービスとしてのデータベース，つまりクラウドデータベースとして抽象化している．その上で，従来あまり研究が行われてこなかった，クラウドデータベースへの問合せからの情報漏洩問題を対象として，次の三つの視点からその安全性に取り組んだ．第一は，サーバへの問合せ内容そのものの安全性であり，第二は，第一の条件の上で動作するアクセス制御である．また，第三は，利用者の関係性や組織に関する情報の安全性である．それぞれに対する本研究の成果は次の様にまとめられる．

第一に，問合せ内容を秘匿したまま目的のデータを取得するプライベートな問合せ手法を開発した．高度なセキュリティを保証する暗号化データベースと言われる既存技術では，問合せに平文の値が含まれないという点でサーバを含む第三者から問合せ内容を秘匿した問合せを実現していた．しかし，攻撃者が問合せの頻度に関する情報を得ている場合，上記既存手法では平文の値を推測する頻度分析攻撃が可能である．本論文で提案する新しい手法では，問合せに摂動を加え暗号化を施すことで頻度分析攻撃を防ぐ問合せを実現した．本手法は摂動に用いる乱数を，平文問合せの分布を考慮して選ぶことにより，平文問合せの分布との相関が低い問合せを実現している．評価実験により本手法による問合せと平文問合せとの相関が十分小さいことが観測され，本手法の有効性を示すことができた．本手法は，クラウドデータベースで要求される問合せのうち，一致問合せ，範囲問合せ両方に対応でき，適用範囲の広い手法となっている．

第二に，暗号化データベースにおける権限不適合が少ないクライアントベースのアクセス制御手法の研究を行った．上記の第一の提案手法などを用いサーバを含む第三者から問合せ内容を秘匿した場合，従来サーバが提供してきたアクセス制御機構を利用することができなくなる．従ってクライアントベースでアクセス制御の仕組みを実現する必要がある．既存のクライアントベースのアクセス制御では，アクセス権限を持たないデータまでを取得しクライアント側でそれらを除去する必要が

あった．この方式では，通信コストやクライアント側の計算コストが大きくなってしまう．本論文で提案するクライアントベースのアクセス制御では，複数のデータベースを用意しアクセス権限が似ているデータのクラスタリングを行うことで，権限ミスの少ないアクセス制御を実現した．また，評価実験により，従来手法に比べて高い権限適合率を達成することを示している．

第三に，問合せログ解析から利用者の類似度計算を防ぐ動的な問合せの書き換え手法を開発した．サーバへの問合せは，利用者の個人情報だけでなく，共通興味を持つ利用者など利用者の潜在的なグループに関する情報も含んでいる．しかし，これまで，こうした利用者の潜在的なグループに関する安全性はほとんど議論されてこなかった．本論文では，攻撃者による問合せ解析から，潜在的なグループの解析に必要な共通の問合せを行った利用者集合を計算する具体的な攻撃方法を示すと共に，その攻撃を防ぐ問合せ方法を提案した．本手法では，拡張可能ハッシュという動的に変化するデータ構造を用いることで，その時点で最適な匿名化を実現した．また，評価実験により導入した攻撃方法が利用者のグループ情報の推定に有効であること，及び提案手法を用いることで攻撃者が攻撃の成否判定を困難にすることが可能であることを示した．　本手法は，サーバに保存されているデータ形式を仮定していないため，　データベースサービスに加え検索エンジンなどにも応用することができるという特徴がある．

これら三つの提案手法は，共にサーバに対して特殊な機能を仮定していないという特徴がある．そのため，今まで蓄積されたサーバ側の技術と組み合わせて利用することが可能であり適用範囲の広い手法となっている．

注)論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせ
て、３，０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１，１００wordsで作成し
審査結果の要旨は日本語５００～２，０００字程度で作成すること。

（続紙　２　）

（論文審査の結果の要旨）

本論文は，アウトソーシングデータベース，いわゆるクラウドデータベースにおいて，問合せからの情報漏洩問題を扱っている．検索エンジンをはじめ，多くの情報サービスでは問合せ履歴を収集することで利用者の行動を解析していることを考えると，本論文は現代の重要な問題に取り組んでいるといえる．

問合せ内容を秘匿したまま目的のデータを取得するプライベートな問合せ手法では，従来の問合せ暗号化だけでは不十分であった頻度分析攻撃に対応するために平文問合せの頻度に応じて摂動に用いる乱数を選択する新たな方法を考案した．この手法により，一致問合せと範囲問合せに対してプライベートな問合せを実現している点で新規性が高い．また，実験により平文問合せと乱数の相関が低いことも示しており，有用性が認められる．さらに提案手法は，プライベートな問合せ手法だけに限らず，サーバに内容を秘匿したまま演算を行わせる問題に対して応用可能であり，適用範囲の広い方式を提案している．

暗号化データベースにおける権限不適合が少ないクライアントベースのアクセス制御手法では，既存のアクセス制御法では扱われていないクライアントベースアクセス制御を効率的に実行するため，クライアントがサーバから取得したデータの権限不適合という新しい問題を導入している点に新規性が認められる．また，権限不適合が少ないアクセス制御方式として，従来はアクセス制御において利用されることがなかった放送暗号の応用とデータベース割り当てという二つの概念を用いて新たな手法を提案している点も評価できる．さらに，権限適合率という尺度を用いて本手法が高い適合率を達成することを示している点も有効性の点から評価できる．

問合せ履歴解析から利用者の類似度計算を防ぐ動的な問合せの書き換え手法では，利用者個人に関する情報の安全性に加え，利用者間の関係に関する情報の安全性について議論している．攻撃者による問合せ解析により共通の問合せを行った利用者集合を計算し利用者の潜在的なグループを解析する具体的な攻撃方法を示すと共に，そのような攻撃に対処するための問合せ方法の提案を行った点は，既存の安全性の研究にはない新たな領域への展開を行った新規性の点で評価できる．提案された問合せ方法は，動的なデータ構造を用いることにより変化していく利用者間の関係を反映させており実用性の面で評価できる．また，実験により上述の攻撃が実際に可能であり，また，問合せ結果を利用者が処理するためのコストとのトレードオフのもとに耐攻撃性実現可能性を示した点が評価できる．

このように，本論文はクラウドデータベースにおいて従来あまり議論されてこなかった問合せからの情報漏洩問題に取り組んだものであり，その新規性と有用性が高く評価される．

よって，本論文は博士（情報学）の学位論文として価値あるものと認める．

また，平成２４年２月９日に実施した論文内容とそれに関連した試問の結果合格と認めた．

注)論文審査の結果の要旨の結句には，学位論文の審査についての認定を明記すること．

更に，試問の結果の要旨（例えば「平成　年　月　日論文内容とそれに関連した口頭試問を行った結果合格と認めた．」）を付け加えること．

Webでの即日公開を希望しない場合は，以下に公開可能とする日付を記入すること．

要旨公開可能日：　　年　　月　　日以降