氏名(本籍・生年月日)　中 村 伸 一(愛知県　昭和４６年３月２９日)
学位の種類　博　士（工 学）
学位記番号　乙 第 ２３１ 号
学位授与の日付　平成２６年９月３０日
学位授与の要件　信州大学学位規程　第５条第２項該当
学位論文題目　暗号化に対応したXML文書検索手法に関する研究
論文審査委員　主査　教　授 山本博章　　准教授 新村正明
教　授 海尻賢二
教　授 和﨑克己
准教授 金子美博（岐阜大学）

論 文 内 容 の 要 旨

インターネット回線の高速化と安定性の向上に伴い，インターネットを介してサーバやストレージ等を提供する，クラウドと呼ばれるサービスが始まっている．クラウドは，運用開始までの時間が短い，性能の増強が容易である，運用に必要な人件費が少ない等から多くの組織で利用されている．

クラウドで利用されるサーバは，専門の施設で管理者によって複数のサーバを集約して運用されるが，利用者と専門の施設が地理的に離れている，クラウドのセキュリティ方針により利用者が専門の施設に入ることができない等から，利用者がサーバと管理者を管理するのは難しい．そのため，クラウドにあるデータのセキュリティを確保しつつ利用できるように，データを暗号化したままで検索する手法が求められるようになってきている．

そのため，本論文ではデータを暗号化したままで検索する手法を紹介する．特に，インターネット上における情報交換に利用されているデータ形式であるExtensible Markup Language(以下XML)に対する暗号化に対応した検索手法について研究している．

主要な商用データベースのデータを暗号化したままで検索する手法は，データを暗号化してファイルに登録しておき，検索する時は暗号化した条件とファイルをメモリ上で復号して検索するように実装されている．しかし，この実装はデータベースのファイルの盗難に主眼を置いており，メモリ上のデータの読み取りについて考慮されていない．従来はデータベースを組織内で構築していたため，利用者が管理者とサーバを管理しやすく前者の検索手法でもセキュリティを確保することができた．しかし，データベースをクラウドで利用する場合，利用者がサーバと管理者を管理するのが難しくなるため，メモリ上のデータの読み取りのような高度な手法の対応が必要となっ

てきている．

データベースに暗号化されたXML文書を登録して検索する手法について，暗号化された文字列を検索する手法からXPathを利用したXML文書の検索へ拡張した手法や，キーワードを利用したXML文書の検索手法を暗号化に対応させる手法がある．しかし，どちらの手法も，XML文書の構造を検索に利用しており，XML文書の構造が暗号化されていない．そのため，管理者が同じXML文書を持っていると，構造を利用して検索内容や結果が推測される問題がある．

本論文では，データを暗号化したままで検索する手法のさらなる実用化に向けた課題である，「検索されるXML文書と同じ内容のXML文書を管理者が入手した場合，検索している要素及びテキストの位置と入手したXML文書を突き合わせることで，検索内容と結果が推測される問題」を取り上げ，その解決方法の提案を行う．

データベースに暗号化されたXML文書を登録して検索する課題に対応した手法を2つ提案する．1つ目はXPathを用いた検索手法の提案である．XML文書におけるXPathにマッチする部分の検索にあたっては，事前にXML文書を暗号化してデータベースに登録する．検索する場合は，データベースからXPathの一部の要素と構造が同じ部分木のデータを暗号化したまま取得し，取得したデータを復号してXPathとマッチするか判定する．2つ目はキーワードを用いた検索手法の提案である．XML文書におけるキーワードの検索にあたっては，事前にXML文書からBloom Filterと暗号化されたデータで構成されたテーブルを構築しデータベースに登録する．検索時はデータベース上でBloom Filterを利用したキーワードによるXML文書の検索を行い，検索結果のBloom Filterに対応する暗号化されたデータをデータベースから取得する．取得した暗号化されたデータを復号して検索結果を作成する．どちらの手法も想定される攻撃に対する安全性を分析し手法が安全であることを示した．

従来の手法との性能比較について，XPathを用いた検索手法はXML文書作成ソフトウェアで作成したXML文書で，提案手法と従来の手法との性能比較を行い，提案手法が対応するXPath の問い合わせ範囲において，一部の問い合わせ以外は高速である結果となった．今後の課題はXPath の問い合わせ範囲の拡張の提案である．キーワードを用いた検索手法は，XML 文書作成ソフトウェアで作成したXML文書で，提案手法と従来の手法との性能比較を行い，検索時間は従来の手法より遅い結果となった．今後の課題は検索時間の高速化である．