平成26年度 情報工学コース卒業研究報告要旨

関 研究室	氏　　名	上 杉　正 紀
卒業研究題目	XMLデータベースに対する木問合せのk-安全性検査法の拡張	

データベースには多くの場合，機密情報が含まれている．機密情報の漏洩を防ぐ一般的な手法としてアクセス制御がある．アクセス制御とは，データベースに対し，機密情報を得るような問合せの実行をアクセス権を持つユーザのみに許可するというものである．以下では，問合せを許可問合せと禁止問合せに分割することによりアクセス制御を行うと仮定する．

しかしながらアクセス権を持たないユーザでも，許可問合せとその問合せ結果とを組み合わせて機密情報（禁止問合せの結果）を推論できることがある．これを推論攻撃と呼ぶ．推論攻撃で漏洩する情報は一般的に自明でない．したがってデータベース管理者は推論攻撃によって機密情報がどの程度漏洩してしまうのかを定量的に把握して安全性を確保すべきである．

情報漏洩に対する量的尺度の一つとしてk-安全性がある．データベースX，スキーマA，禁止問合せQ_s，n個の許可問合せ$Q_1,...,Q_n$を仮定する．スキーマAを満たすようなデータベースの集合$L(A)$と，許可問合せ$Q_1,...,Q_n$の結果$Q_1(X),...,Q_n(X)$からそれぞれ推論されるデータベースの集合$Q_1^{-1}(Q_1(X)),...,Q_n^{-1}(Q_n(X))$の共通部分から得られる禁止問合せ$Q_s$の結果の候補数$|Q_s(L(A)\cap Q_1^{-1}(Q_1(X))\cap ...\cap Q_n^{-1}(Q_n(X)))|$が$k$個以上存在するとき，すなわち禁止問合せ$Q_s$の結果が$k$個未満に絞り込めないときに，データベース$X$は$k$-安全であると定義される．許可問合せが一つで禁止問合せとスキーマが指定されていないという単純な場合，つまりデータベースの候補数$|Q_1^{-1}(Q_1(X))|$がk個以上であるときにデータベースXがk-安全であると定義する場合について，k-安全性を判定する手法が提案されている．この手法では，許可問合せQ_1の入出力関係を充足可能性問題に帰着し，命題論理式のモデル（命題論理式を充足するような，論理変数への真偽値割り当て）を数えることによりk-安全性を判定する．

本研究では，上述のk-安全性検査法の拡張を行った．既存のk-安全性検査法では，一つの問合せとその問合せ結果から元のデータベースを推論すると仮定していた．本研究における手法では，データベースに適合するスキーマ，複数の許可問合せとその問合せ結果から禁止問合せの結果を推論すると仮定し，k-安全性の検査を行う．データベースはXMLデータベースを木構造データとして扱う．問合せには木問合せとして木変換器の部分クラス（操作として部分木の削除，ラベルの付け替えのみを持つ）を考える．スキーマは木オートマトンで与える．k-安全性検査の手順としては，まずスキーマ適合性制約，許可問合せの入出力関係制約，禁止問合せの入出力関係制約を制約式として表現する．次に制約式を順序符号化を用いて命題論理式に変換し，最後に命題論理式のモデルを数え，k-安全であるかどうかを判定する．

また本研究では，拡張したk-安全性検査法に基づいたk-安全性検査システムを実装し，国勢調査データを用いて実装システムの実験，評価を行った．実験の結果，既存のk-安全性検査法より強力な攻撃者を想定してk-安全性の判定を行えることが分かった．またデータベースのレコード数，属性数，許可問合せを変化させて，実装システムがk-安全性検査に要する実行時間と使用メモリ量を計測した．その計測結果に基づき，提案手法の有効性と解決すべき課題について考察した．