# 平成25年度 情報工学コース卒業研究報告要旨

| 関 研究室 | 氏　　名 | 浅 井 孝 俊 |
|---|---|---|
| 卒業研究題目 | モデル計数ツールを用いた木問合せのk-安全性検査法 | |

近年、企業等多くの組織でデータベースが運用されている. それらのデータベースには多くの場合に機密情報が含まれており, それらの情報の安全性を守ることの重要性は高い. 機密情報の漏洩を防ぐための一般的な手法としてアクセス制御がある. これはアクセス権のあるユーザーに対してのみ機密情報を得ることのできる問合せの実行を許可するというものである. しかし, 許可された問合せとその出力を組み合わせて推論することでデータベース内の機密情報を得ることが可能な場合がある. この攻撃は推論攻撃と呼ばれる. 推論攻撃で漏洩する情報は一般的に自明でないため, 安全性確保のためには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するかを定量的に把握しておくことが重要である.

推論攻撃等で発生する情報漏洩に対するセキュリティの尺度として非干渉性がある. これは, あるプログラムPに機密情報Xを与えた時に得られる出力YからXに関する情報が一切得られないというものである. ただし現実のプログラムが入力Xに対して意味のある動作を行い出力をしている以上, 非干渉性という尺度だけで現実のプログラム全てに対応することは難しいと考えられる. このような背景から近年，情報漏洩もしくは情報流の量的尺度が注目されている．これは出力が機密情報をどの程度含んでいるかという尺度で評価する方法である. その量的尺度の1つにk-安全性がある. あるプログラムPと機密情報Xがあった時にPによって得られた出力YからP(X) = Yとなる入力候補Xがk個以上存在するとき, すなわちk個未満に入力候補を絞り込めないときにプログラムPは出力Yに対してk-安全であると定義される.

本研究ではモデル計数ツールを用いた木問合せに対するk-安全性検査法を提案する. 木問合せとは入力および出力が木構造であるような問合せである．XML文書を代表とする構造化データは木構造でモデル化することができ, このような構造化データからなるデータベースへの問合せは木問合せによってモデル化することができる．提案手法では出力と入力候補木との関係が問合せを満たすかという問題を論理式で表現し, その論理式を充足するモデル (論理変数への真偽値割当て) を数えることでk-安全性を検査している. データベース及び出力はXML文書であり木構造として扱う. また問合せは一般的な木問合せモデルであるXSLTの形式モデルの一つである, 線形決定性ボトムアップ木変換器の部分クラス (deleting,relabelingのみ) とする. 提案する手法ではまず, 与えられた木問合せと出力木から, 入力候補木, 変換中の状態を記録する木,deleting,relabelingのラベルを記録する中間木の3つが問合せの変換規則によって関係づけられるか, また実際に得られた出力木と中間木の関係が満たされているかを表している論理式を作成する. 次にその論理式を順序符号化を用いることでCNF(Conjunctive Normal Form)に変換し, 最後にCNF論理式を満たす入力木に対応する論理変数への真偽値割当て (モデル) の数を数える.

本研究では更に, 上で示した手法に基づいたツールを実装した上で, いくつかのサンプルを与え実行時間および作成されるCNF論理式の節, 変数の数を記録し, それに基づいて提案手法の有効性を評価した.