平成25年度 情報工学コース卒業研究報告要旨

結縁・寺内 研究室	氏　　名	山 本　真 輝
卒業研究題目	実行ログを用いた量的情報流解析	

プログラムの情報流出は重要な問題である．プログラムによる情報流出はバグや人為的要因が主なものであるが，正常な動作をしているプログラムであっても情報を流出してしまうことがある．機密情報を持つプログラムは，内部の処理の結果としての出力が機密情報に依存することがある．そのため，出力値から機密情報を推定することができ，悪意のある攻撃者がプログラムの出力を観測することによって情報漏洩につながってしまう．このためプログラムの出力が持つ情報量を解析することはセキュリティにおいて大きな意味を持つ．

機密情報と攻撃者が観測可能な出力の依存関係をもとに機密情報がどの程度漏洩するかという考えが量的情報流である．量的情報流の解析においてある実数 q を用いて量的情報流が q 以下で抑えられるということを量的情報流の上限問題という．上限を求めることにより，プログラムを実行した際に出力を観測することによって漏れる情報は多くても q であるということが出来るため，プログラムの安全性を表す尺度とすることが出来る．

量的情報流の定義は複数存在する．そのうちの 1 つに「Belief に基づく量的情報流」がある．これは攻撃者がプログラムの機密情報を予測したときの量的情報流である．この予測の分布を belief という．Belief に基づく量的情報流は，機密情報を入力した際の出力と同じ出力になる入力の個数と belief を用いて計算することが出来る．

既存の量的情報流を求める手法には，適用できるプログラムが小さいプログラムに限られるといった問題点が存在する．

本研究では実行ログの解析を行うことによってプログラムの量的情報流の上限を求める新たな手法を提案する．プログラムの実行ログを解析し最弱事前条件を求め，その式が充足する値の個数を調べることによって量的情報流の上限を求める．プログラムから実行ログを取ることにより，適用できるプログラムが小さいものに限られるという問題を解決する．

本研究ではこの手法を用いるために，プログラムを実行した際に実行ログを取ることができるようにプログラムの書き換えを行うプログラム変換器の実装を行う．また，実行ログを解析するための解析器の実装も行う．作成した解析器を用いることにより最弱事前条件を求め，式が充足する値の数を求めることが出来る．その値を利用して量的情報流の上限を計算することができることを示す．