別紙１－１

論文審査の結果の要旨および担当者

報告番号	※　甲　第　　号

氏　　名　　CHU Bao Trung

論　文　題　目

Towards Practically Applicable Quantitative Information Flow Analysis

（実用化を目指した量的情報流解析に関する研究）

論文審査担当者

主　査　　名古屋大学教授　関　　浩之

委　員　　名古屋大学教授　結縁　祥治

委　員　　名古屋大学准教授　西田　直樹

委　員　　名古屋大学教授　楫　　勇一（情報戦略室）

別紙１－２

論文審査の結果の要旨

プログラムの量的情報流（Quantitative Information Flow，QIF と略す）とは，プログラムの出力値を観測することによって機密入力値に関する情報がどれだけ得られるかを表す量的尺度であり，ソフトウェアの脆弱性の指標として用いられる．しかし，従来の QIF は，すべての出力値に関する漏洩量の期待値と定義されており，特定の出力値を観測したときに大きな漏洩が生じる場合でも QIF 自体は小さい値になる場合がある．そこで，個々の実行における出力値に基づく QIF（動的 QIF とよぶ）の妥当な定義を与え，動的 QIF の効率的な計算法を究明することが課題となっていた．このような背景のもと，本研究では動的 QIF の具体的な定義を提案しその妥当性を考察するとともに，動的 QIF 解析の計算量の理論的評価，および，動的 QIF の計算効率を向上させる手法の提案とその有効性の実験的評価を行っている．本論文は以下の6章からなる．

第1章では，ソフトウェアの脆弱性を定量化することは現代社会における重要課題であることが実例を用いて説明され，続いて本研究の目的，得られた成果の概要，ならびに関連研究について述べられている．

第2章では，従来の QIF の定義とその計算方法，特に論理式のモデル計数を利用した計算方法について述べられている．

第3章の前半では，動的 QIF の定義として，出力値観測後の機密入力値の自己情報量に基づく指標（QIF1）と，機密入力値と出力値の同時情報量に基づく指標（QIF2）の2つが提案され，それらの定義の妥当性と特性が議論されている．理論的考察として，ブールプログラムの QIF1 と QIF2 の計算問題に付随する判定問題の計算量を明らかにしている．さらに，既存のモデル計数ツールを活用してこれらの動的 QIF を計算するツールを実装し，ベンチマークプログラムを用いて計算実験を行った結果が述べられている．第3章の後半では，プログラムの動的 QIF を計算するとき，より規模の小さいプログラムに分解し，分解された部分プログラムの QIF の計算結果からもとのプログラムの QIF を得る手法として，プログラムの入出力値集合を分割する手法（ValDo）とプログラム構造を直列分解する手法（Seq）を提案している．ValDo は QIF 計算の並列化に適し，Seq はプログラムがいくつかの直列フェーズに分解可能な場合に効果が大きいことが実験的に示されている．

第4章では，文字列を扱うプログラムを対象とし，認識可能級数と代数的級数に対する計数問題を導入してこれらの問題を効率良く計算するアルゴリズムを提案するとともに，その基本的な有効性が試作システムを用いた実験により示されている．

第5章では，QIF 解析におけるデータ循環について論じてられており，2つの循環を導入した新しいモデルが提案されている．

第6章では，本論文の総括ならびに今後の研究課題について述べられている．

以上の通り，本論文はコンピュータセキュリティ，特にソフトウェアの脆弱性を定量化するための適切な尺度の導入とその効率的な計算法を示しており，提出者の CHU Bao Trung 氏は博士（情報科学）の学位を受けるのにふさわしいと判断する．