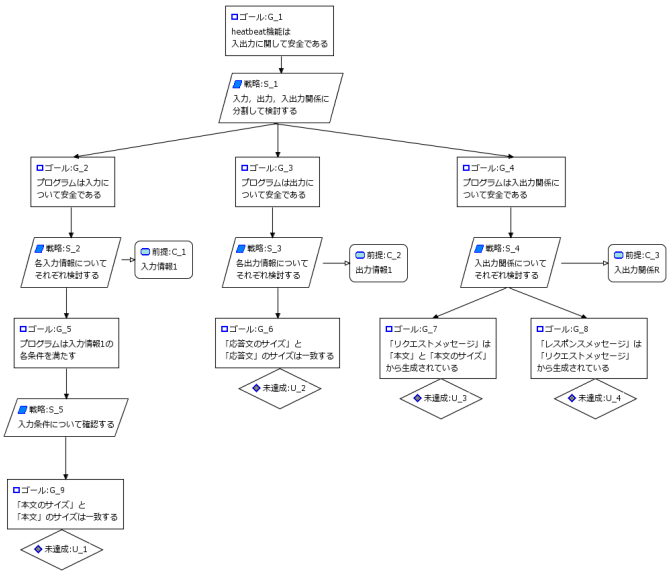
平成27年度 情報工学コース卒業研究報告要旨

山本 研究室	氏　　名	宮 林　凌 太
卒業研究題目	入出力分析に基づくコード保証方法	

今日の情報社会では，ソフトウェアの安全性を高めることが求められている．要求を満足するように，記述されたプログラムコードによってソフトウェアが実行される．コードの安全性がソフトウェアの安全性に直結するため，テストによってコードに欠陥がないことを確認した上で，リリースされる．しかし，テストでコードに欠陥が見つかれば手戻りが発生する．この手戻りを抑止するとともに，コードの安全性を高める手法として，静的解析ツールを用いたソースコードの検査手法や人手によるコードレビュ手法がある．しかし，前者では解析結果の警告が高い false-positive 率を持つため，解析結果の確認作業の負担が高くなる．後者では，レビュ基準が明確になっておらず，レビュ担当者によって不具合箇所の検出精度が異なるという問題がある．

そこで，本研究では各モジュールの入出力仕様に着目した分析から，コードの安全性を保証するコード保証方法を提案する．提案手法では，まず仕様書から入力に関する制約条件，入出力の関係，出力に関する制約条件，という入出力情報を作成する．その入出力情報を基に，入出力に関するコードの保証ケースを記述する．保証ケースは GSN(Goal Structuring Notation) という議論をモデル化するための表記法に準拠しており，左図に示すように記述する．保証ケースを提案手法で導入する理由は，議論を木構造で図式化でき理解を容易化できる点と，要求に対する実装コードが存在することを証拠に基づいて論証できる点にある．保証ケースでは，示したい主張としての要求に対して対するコードを証拠として付与することで，議論の正当性を示すことができる．提案手法では，この証拠としてソースコード中の該当箇所を対応付ける．具体的には，GSN で示した証拠に付与した ID をソースコード中のコメントに付与することで対応関係を表現する．



保証ケースの例

提案手法の評価を行うために，実際のオープンソースソフトウェアの OpenSSL における公表済みの 2 つの脆弱性 (HeartBleed,FREAK) を対象に，提案手法の適用実験を行った．適用実験では対象とする仕様書とプログラムコードから，提案手法を用いて実際の脆弱性につながりうる欠陥を発見できることを確認した．適用実験の結果，提案手法では 2 つの OpenSSL の脆弱性に対して，それぞれの脆弱性につながる欠陥を発見した．

現状の提案手法は入出力の処理内容については考慮していない．このため，入出力処理を考慮できるように提案手法を拡張し，有効性を確認することが今後の課題である．