様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　　９　日現在

機関番号：　３４３１５
研究種目：　若手研究(B)
研究期間：　2012～2014
課題番号：　２４７０００３６

研究課題名（和文）情報流解析と型エラースライシングに基づくソフトウェアの安全性検証と開発支援

研究課題名（英文）Verification and Development Environment of Secure Software using Information Flow Analysis and Type Error Slicing

研究代表者

桑原　寛明（Kuwabara, Hiroaki）

立命館大学・情報理工学部・助教

研究者番号：３０４３２２２２

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：本研究では、情報流解析を対象とする型エラースライシングの正当性を証明した。加えて、非機密化プリミティブの配置手法を提案した。型エラースライシングと非機密化プリミティブはいずれも機密情報を漏洩しないソフトウェアの開発支援手法である。さらに、開発者が統合開発環境上で行った操作履歴に基づいてコード補完を改善して開発作業を支援する手法を提案した。

研究成果の概要（英文）：We proved the soundness of type error slicing for information flow analysis and proposed a method of declassifiers placement in information flow analysis. Both type error slicing and declassifiers placement are methods to support development of secure software that do not leak secret information. Moreover, we proposed an improvement of code completion of integrated development environment using editing operation history.

研究分野：　ソフトウェア工学

キーワード：　情報流解析　型システム　型エラースライシング　ソフトウェア開発支援

１．研究開始当初の背景

我々の身の回りでは様々なソフトウェアが稼動しており、その中には機密データを扱うソフトウェアも少なくない。そのようなソフトウェアは機密データを外部に漏洩させないことが重要である。そのため、ソフトウェアが正常な動作としてどのように振舞っても機密データが漏洩しないことを網羅的に検査する手法として、型システムを用いた情報流解析の手法が提案されている。しかし、情報流解析に基づくソフトウェアの検査は現実にはほとんど行われていない。その理由として、検査がコンパイラや開発環境に組み込まれていないため気軽に利用できないこと、検査に失敗した場合にその原因箇所がわかりにくいことが挙げられる。

情報流解析に基づく検査は、ソフトウェアの質の向上には貢献するがソフトウェアの動作には影響しない。検査に失敗しても見かけ上ソフトウェアは正常に動作しているように見えるため、検査が重要視されない傾向が強い。検査に失敗した原因の特定が難しい場合は開発者がその失敗を無視し、さらには検査自体を省略しがちである。情報流解析に基づく検査が有効に活用されるためには、検査を開発環境に組み込んで強制するとともに、検査に失敗した場合に失敗の原因箇所を提示し修正を促すことが必要である。

２．研究の目的

本研究では、正当性が保証された情報流解析と型エラースライシングに基づく安全なソフトウェアの開発手法を確立することを目的とする。安全なソフトウェアとは、機密データを外部に漏洩するような動作を含まないソフトウェアを指す。情報流解析によってソフトウェアの安全性を保証し、型エラースライシングによって安全なソフトウェアの開発工程を支援する。

本研究では、例外処理付きオブジェクト指向言語を対象とする情報流解析における細粒度な型エラースライシングを提案する。提案する情報流解析に基づく検査が安全でないソフトウェアを安全であると誤判定しないこと、および型エラースライシングが正しくプログラムスライスを計算できることを証明する。さらに、情報流解析と型エラースライシングを統合開発環境へ組込むことで、開発者が開発中のソフトウェアが安全であるか、安全でない場合どこがその原因箇所なのか容易に理解でき、安全でないソフトウェアがリリースされる可能性を低減する。

３．研究の方法

本研究では、情報流解析と型エラースライシングに基づく安全なソフトウェア開発を支援するために以下の項目について研究を進める。

(1) 例外処理付きオブジェクト指向言語向け情報流解析のための型エラースライシング手法の構築
(2) 型エラースライシング手法の正当性の証明
(3) 情報流解析と型エラースライシングの統合開発環境への組込み

統合開発環境への組込みにあたっては、検査対象のプログラムを解析する必要がある。情報流解析と型エラースライシングでそれぞれ異なる解析を行う必要があるため、汎用的なプログラム解析基盤を構築し、解析基盤を用いて情報流解析と型エラースライシングを実現する。

４．研究成果

本研究課題の成果は

(1) 型エラースライシングの正当性の証明
(2) 非機密化プリミティブの配置手法の提案
(3) 編集操作履歴を用いたソフトウェア開発支援手法の提案

である。

(1) 型エラースライシングの正当性の証明

本研究では、手続き型言語向けの情報流解析を対象とする細粒度な型エラースライシングの正当性を証明した。情報流解析は情報の機密度を型とする型システムとして実現され、機密情報を漏洩しないプログラムのみを型付けできる型付け規則から構成される。型エラースライシングとは、型エラーを含むプログラムから型エラーの原因となるコード片のみを抽出することである。情報流解析を対象とする型エラースライシングでは、機密情報の漏洩に関係するコード片が抽出される。型エラースライシングが正当であるとは、抽出されたコード片からなるプログラムが元のプログラムと同じ理由で型エラーとなることを指す。

この結果により、スライスして得られるプログラムに対して修正を行い型エラーを解消することができれば、同じ方法で元のプログラムの型エラーも解消できることが保証される。スライス後のプログラムは型エラーと無関係なコード片を含んでおらず、問題点の理解と修正方法の検討が容易である。そのため、元のプログラムの修正方法をスライス後のプログラムを対象として検討できることは有用である。

(2) 非機密化プリミティブの配置手法の提案

本研究では、不正な情報流を含むプログラムに対して、開発者が許容する不正な情報流を明示するための非機密化プリミティブを配置する手法を提案した。機密情報の直接的な漏洩だけでなく間接的な漏洩も含む不正な情報流をすべて禁止した場合、有用なプログラムを作成することはほぼ不可能である。そのため、一部の不正な情報流を許容する必要があるが、どの不正な情報流が許容できる

かは開発者にしか判断できない。
提案手法では、開発者が許容する不正な情報流を明示するために、非機密化プリミティブを配置すべきプログラム中の箇所の候補を列挙する。プログラム中の適切な箇所に非機密化プリミティブを配置することで情報流解析による検査を成功させることができるが、非機密化プリミティブを必要な箇所に最低限必要なだけ配置することは容易ではない。適切な配置箇所の候補を列挙することで開発者を支援することができる。
情報流解析は型システムとして実現されるため制約充足問題に帰着させることが可能であり、不正な情報流を含むプログラムからは充足不能な制約集合が生成される。提案手法では、充足不能な制約集合に対して Minimal Correction Subset(MCS)を求め、MCS に含まれる制約が由来するプログラム構成要素を非機密化プリミティブの配置箇所の候補とする。この手法により挙げられた候補に従って非機密化プリミティブを配置すれば必ず検査が成功すること、およびこの手法により候補が必ず一つ以上挙げられることを証明した。
情報流解析では、情報の機密度が束構造を構成するが前提である。提案手法では、機密度の束構造には制約を設けず、任意の束構造に対応している。非機密化プリミティブを配置する際には新しい機密度を指定する必要があるため、新しい機密度を求める手法を提案した。さらに、この手法により求められる新しい機密度が検査を成功させることが可能な最大の機密度であることを証明した。

(3) 編集操作履歴を用いたソフトウェア開発支援手法の提案
本研究では、プログラム解析基盤の応用として、開発者の編集操作履歴を用いたソフトウェア開発支援手法を提案した。具体的には、編集操作履歴の効果的な再生手法、および編集操作履歴を用い効果的なコード補完候補の列挙手法を提案した。編集操作履歴とは、開発者が統合開発環境上で行った操作の記録である。文字の挿入や削除といったエディタ上で行われる操作だけでなく、ファイルの保存やメニューの選択によるコマンド実行などあらゆる操作が記録される。
記録された編集操作履歴を再生することで、ソースコード編集の過程や開発者が行った操作を分析できる。しかし、編集操作履歴は細粒度な履歴であるため、用途に対して過度に詳細である場合も多い。そこで、操作のフィルタリングや融合、グループ化によって履歴の粒度を粗くする手法を提案した。操作のフィルタリングは、着目したい操作のみを含む履歴を生成する。操作の融合は、履歴中の連続する文字列編集操作を最終結果の文字列を挿入あるいは削除する一つの操作に合成する。操作のグループ化は、履歴中の連続する複数の操作を意味のあるかたまりに分解する。これらにより、ソースコード編集の概観や履歴内の検索を容易に行うことができる。
統合開発環境を用いたソースコード編集ではコード補完機能が多用され、ソースコードの効率的な入力が実現されている。コード補完では、実際に入力されるコード片が候補の上位に挙げられると最も効果的であるため、編集操作履歴に記録されたコード補完の繰り返しに基づいて候補を並び替える手法を提案した。提案手法では、入力されるコード片が同じコード補完は短い間隔で繰り返される傾向が強いことを編集操作履歴の調査から明らかにし、直近に行われたコード補完で入力されたコード片を候補の上位に表示する。

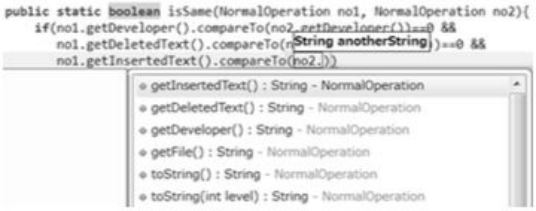

図 1　提案手法によるコード補完例

提案手法を Eclipse のコード補完機構に組み込んで実験を行い、提案手法が従来のコード補完よりも適切な候補を上位に挙げることを確認した。

まとめと今後の課題
本研究では、情報流解析に基づく安全なソフトウェア開発の支援手法について研究を行った。型エラースライシングだけでなく、非機密化プリミティブの配置手法へと研究が進展した。
手法の正当性の証明は進みつつあり、今後は具体的な開発支援ツールとして実現する予定である。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　3 件）
(1) 桑原寛明, 國枝義敏. 情報流解析における Declassifier の配置手法. コンピュータソフトウェア, Vol.32, No.1, pp.136-146, 10.11309/jssst.32.1_136, 査読有, 2015.
(2) Takayuki Omori, Hiroaki Kuwabara and Katsuhisa Maruyama. Improving code completion based on repetitive code completion operations. コンピュータソフトウェア, Vol.32, No.1, pp.120-135, 10.11309/jssst.32.1_120, 査読有, 2015.
(3) 桑原寛明, 大森隆行. 編集操作履歴の再

生における粗粒度な再生単位. コンピュータソフトウェア, Vol.30, No.4, pp.61-66, 10.11309/jssst.30.4_61, 査読有, 2013.

〔学会発表〕(計 7 件)

(1) 渥美紀寿, 桑原寛明. 静的検査ツールにおける警告箇所の版間追跡による確認コスト削減手法. 情報処理学会研究報告, 2015/03/13, 化学会館, 東京都.
(2) 渥美紀寿, 桑原寛明. 変更追跡機能を用いた静的検査ツールの効果的な利用法. ソフトウェア工学の基礎 XXI (FOSE 2014), 2014/12/12, 霧島国際ホテル, 鹿児島県.
(3) 桑原寛明, 國枝義敏. 任意の機密度束を用いた情報流解析における非機密化プリミティブの配置. ソフトウェア工学の基礎 XXI (FOSE 2014), 2014/12/12, 霧島国際ホテル, 鹿児島県.
(4) 桑原寛明, 國枝義敏. 情報流解析における Declassifier の配置手法. ソフトウェア工学の基礎 XX (FOSE 2013), 2013/11/28, ゆのくに天祥, 石川県.
(5) 桑原寛明, 大森隆行. 編集操作履歴の再生における粗粒度な再生単位. ソフトウェア工学の基礎 XIX (FOSE 2012), 2012/12/15, ゆふいん山水館, 大分県.
(6) 大森隆行, 桑原寛明, 丸山勝久. 統合開発環境におけるコード補完の繰り返しに関する調査. ソフトウェア工学の基礎 XIX (FOSE 2012), 2012/12/14, ゆふいん山水館, 大分県.
(7) Takayuki Omori, Hiroaki Kuwabara and Katsuhisa Maruyama. A Study on Repetitiveness of Code Completion Operations. Proceedings of 28th IEEE International Conference on Software Maintenance (ICSM'12), 2012/09/25, Trento, Italy.

６．研究組織

(1)研究代表者

桑原 寛明 (KUWABARA Hiroaki)
立命館大学・情報理工学部・助教
研究者番号：30432222