様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ５ 月 ２６ 日現在

機関番号：３３９１７
研究種目：若手研究(B)
研究期間：2017～2020
課題番号：１７Ｋ１２６６６

研究課題名（和文）情報流解析による安全性検証に基づく実用的なソフトウェア開発支援

研究課題名（英文）Practical Software Development Support based on Safety Verification using Information Flow Analysis

研究代表者

桑原　寛明（Kuwabara, Hiroaki）

南山大学・理工学部・講師

研究者番号：３０４３２２２２

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：機密データを扱うソフトウェアは、機密データを外部に漏洩させないことが求められる。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る舞っても機密データが漏洩しないことを開発中に検査することが重要である。そのための検査手法として情報流解析が存在するが、本研究では情報流解析を実用的なソフトウェア開発において適用可能とするために必要な拡張を行った。また、情報流解析を適用するために必要な追加情報をJavaプログラム中に記述するための記法を考案して適用可能性を検討した。

研究成果の学術的意義や社会的意義
本研究の成果により、情報流解析の適用対象であるプログラムの記述の柔軟性が向上しており、かつ広く利用されているJava言語における標準的な記法のみを利用して情報流解析のために必要な機密度に関する情報をJavaプログラム中に記述できるため、開発者は機密度の概念と記法を理解すれば情報流解析による安全性検証を開発中のソフトウェアに対して実施できる。ソフトウェアの開発中に安全性検証を行うことができるため、機密データを漏洩する可能性のある安全ではないソフトウェアのリリースが抑制されることが期待できる。

研究成果の概要（英文）：Software that processes confidential data should not leak confidential data to the outside of software. It is important to check during development whether confidential data leak or not in any behavior of the software. In this research, we proposed some extensions of information flow analysis to make it applicable to practical software development. In addition, we defined a notation for describing additional information necessary for applying information flow analysis in Java programs.

研究分野：ソフトウェア工学

キーワード：情報流解析　プログラム解析　安全性検証　ソフトウェア開発支援

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

我々の周囲では様々なソフトウェアが稼働しており、機密データを扱うソフトウェアも数多く存在する。そのようなソフトウェアには扱っている機密データを外部に漏洩させないことが要求されるため、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確認することが重要である。しかし、テストによる網羅的な確認は困難である。この問題に対し、例外処理機構を持つオブジェクト指向プログラムを対象とする型検査に基づく情報流解析が提案されている。型検査に基づく情報流解析は、機密データそのものの漏洩、および機密データの推測に利用できる情報の漏洩がプログラム中に存在しないことを網羅的かつ機械的に検証する手法であり、手法の正当性を数学的に証明可能な型システムとして実現される。

情報流解析の基礎的な理論に関する研究は多く存在し、プログラミング言語の様々な構文に対応した情報流解析のための型システムが構築されている。しかし、情報流解析を実際のソフトウェア開発に応用して実用的なソフトウェアの安全性を検証するためには解決すべき課題が残されている。情報流解析を適用する際には、機密度の種類と大小関係（以下、機密度の構造）を定義し、かつプログラムが扱う各種データについてその機密度を指定する必要があるが、一般的なプログラミング言語にはそのための仕組みが存在しない。実用的なソフトウェアはライブラリを利用するため、従来の研究では考慮されていないライブラリをうまく扱う必要がある。このような課題により、機密データの漏洩に関して情報流解析に基づきプログラムを網羅的に検査することは行われておらず、ソフトウェアの安全性に対する脅威の一つとなっている。

２．研究の目的

本研究では、一般的なプログラミング言語によるソフトウェアに対して情報流解析に基づく安全性検証を行うために必要な要素技術の確立を目的とする。情報流解析に基づく安全性検証の実用性を向上させ、安全なソフトウェアの開発を支援する。

本研究では広く利用されている Java 言語を対象とし､特殊な言語拡張を導入するのではなく、Java プログラムとして標準的な記法のみを利用して情報流解析を実現する。これにより、情報流解析の適用にかかる開発者の負担を低減しつつ、実用的なソフトウェアに対する安全性検証が可能となり、安全なソフトウェアの開発が促進される。安全性検証はプログラムのコンパイル時に実行できるため明示的に起動する必要はなく、検証結果をコンパイル結果の一部として開発者にフィードバックすることや、統合開発環境と連携して視覚化することで開発支援を実現できる。

本研究により、機密データを漏洩する可能性のある安全でないソフトウェアのリリースを抑制できる。外部からの不正な入力に対してソフトウェアが正常に動作した結果として発生する機密データ漏洩事件・事故の多くを回避することが期待できる。

３．研究の方法

本研究では、情報流解析による安全性検証に基づく安全なソフトウェアの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) アノテーションによる機密度の記述法の確立とアノテーション処理系の構築
アノテーションを用いて Java プログラムの一部として機密度の構造と各種データの機密度を記述する方法、およびコンパイル時に実行されるアノテーション処理の一環として記述された機密度に基づいて情報流解析を実行する手法を確立する。

(2) ライブラリを考慮した情報流解析手法の構築
ライブラリを利用するユーザプログラムに対して情報流解析を実行する手法を確立する。ライブラリに対する情報流解析の結果を再利用可能とすることで、同じライブラリを利用するユーザプログラムの情報流解析時にライブラリの再解析を不要とする。

(3) 非機密化に基づくデータ出力機構の構築
情報流解析は機密度の高いデータに依存する出力を安全でないとみなすが、実用的にはそのような出力を許容する必要がある。そこで、開発者が明示した場合に限り機密データを一時的に機密解除する非機密化に基づくデータ出力を Java 言語の仕様を拡張することなく実現する仕組みを構築する。

４．研究成果

本研究課題の主な研究成果は

(1) オブジェクト指向言語の情報流解析における機密度パラメータ

(2) 制約付き機密度パラメータ

(3) 機密度ワイルドカード
(4) 機密度パラメータおよび機密度ワイルドカードのための Java アノテーション
(5) Rust プログラムに対する情報流解析のための型システム
である。

(1) オブジェクト指向言語の情報流解析における機密度パラメータ
オブジェクト指向プログラムを対象とする情報流解析における機密度パラメータを提案した。機密度パラメータは、データ構造の一部を構成するデータの機密度を具体的な機密度ではなくパラメータとして記述するための仕組みであり、Java 言語におけるジェネリクスを機密度に対して適用したものと考えることができる。機密度パラメータを用いることで、コレクションフレームワークのように扱うデータの機密度を定義時には決定できないクラスを定義することができる。クラスの利用時に機密度パラメータに対して具体的な機密度を割り当てる。
本研究では、クラスベースのオブジェクト指向言語においてクラス内に記述される機密度をパラメータ化できるクラスを用意し、機密度パラメータも機密度の一種として扱えるように拡張された機密度束に基づいて型システムを定義した。本型システムによって型付けできるクラスは、機密度パラメータにどのような機密度が割り当てられても非干渉性を満たすことを証明した。

(2) 制約付き機密度パラメータ
型検査に基づく情報流解析における制約付き機密度パラメータを提案した。機密度パラメータを用いることで、各データの具体的な機密度を指定することなくクラスや関数を定義できるが、機密度パラメータに対して具体的な機密度をどのように割り当てても非干渉性を満たすことが要求される。この要求は、プログラムを記述する上での柔軟性を妨げる強い制約であり、緩和する必要がある。
制約付き機密度パラメータは、機密度パラメータに対して割り当てることができる機密度の条件を記述するための仕組みであり、任意の機密度ではなく条件を満たす機密度が割り当てられた場合に限り非干渉性を満たすことを要求する。本研究では、制約付き機密度パラメータを扱うことができる情報流解析のための型システムを定義し、非干渉性に対する健全性を証明した。以上により、制約付き機密度パラメータを用いることでプログラム記述の柔軟性が向上すると同時に、型付け可能なプログラムは不正な情報流を含まないことが保証される。

(3) 機密度ワイルドカード
型検査に基づく情報流解析における機密度ワイルドカードを提案した。機密度がパラメータ化されたクラスは不変(invariant)である、すなわちクラス C<X>の機密度パラメータ X に異なる機密度 L と H を割り当てた C<L>と C<H>は L と H の関係に関わらず常にサブタイプ関係が成り立たないため、柔軟な API の実現が難しい場合がある。機密度ワイルドカードはこの問題を解決する。
本研究では、特に、機密度がパラメータ化されたクラスがメソッドの仮引数の型に出現する場合に着目して、境界付きの機密度ワイルドカードのための構文、機密度ワイルドカードを含む機密度の大小関係とデータ型のサブタイプ関係、情報流解析のための型システムを定義した。以上により、機密度がパラメータ化されたクラスを用いた柔軟な API が実現できる。なお、定義した型システムの非干渉性に対する健全性の証明が今後の課題となっている。

(4) 機密度パラメータおよび機密度ワイルドカードのための Java アノテーション
情報流解析を適用するためには、対象のプログラムに出現する変数などの機密度を指定する必要がある。既存研究において、広く利用されている Java プログラムに情報流解析を適用するために、Java プログラム内に機密度を記述するためのアノテーションを提案しており、これを機密度パラメータおよび機密度ワイルドカードを扱えるように拡張を行った。
従来定義されていた機密度束の定義を示すためのアノテーションと機密度を指定するためのアノテーションに、機密度パラメータの宣言、機密度パラメータに対する機密度の割り当て、機密度パラメータに対する機密度ワイルドカードの割り当てのためのアノテーションを新たに定義した。Java アノテーションの仕様上の制約と記述の容易性が考慮された定義となっている。なお、新たに定義したアノテーションの処理系と統合開発環境への組込みは今後の課題である。

(5) Rust プログラムに対する情報流解析のための型システム
Rust プログラムに対する情報流解析のための型システムを提案した。Rust 言語はシステムプログラミングのためのプログラミング言語であり、Web ブラウザエンジンの開発などに利用されている。メモリ安全性を静的に保証するための言語機能を備えていることから注目を集めており、今後広く利用される可能性がある。このようなプログラミング言語に対して、機密情報保護の観点からプログラムの安全性を検証する情報流解析を実現することは重要であるため、当初の研究計画には含まれていなかったが取り組むこととした。
本研究では、Rust のメモリ安全性に関わる言語機能を抽出したサブセット言語を定義し、サブセット言語を対象として情報流解析のための型システムを構築した。また、サブセット言語の

操作意味を定義し、型システムが非干渉性に対して健全であることを証明した。本研究ではサブセット言語が対象であり、フルセットの Rust 言語に向けて拡張することが今後の課題である。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 長谷川 健太、桑原 寛明、國枝 義敏	４．巻 37
２．論文標題 Java Stream APIによるストリーム操作の停止性検査のための型システム	５．発行年 2020年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 2_59～2_75
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.2_59	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 桑原 寛明, 國枝 義敏	４．巻 36
２．論文標題 情報流解析における制約付き機密度パラメータ	５．発行年 2019年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 4_39～4_45
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.36.4_39	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 吉田 真也, 桑原 寛明, 國枝 義敏	４．巻 36
２．論文標題 オブジェクト指向言語の情報流解析における機密度のパラメータ化	５．発行年 2019年
３．雑誌名 コンピュータソフトウェア	６．最初と最後の頁 48-65
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.36.48	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 桑原 寛明
２．発表標題 情報流解析における機密度ワイルドカードの検討
３．学会等名 FOSE 2020
４．発表年 2020年

１．発表者名
長谷川 健太, 桑原 寛明, 國枝 義敏

２．発表標題
Rustプログラムの情報流解析のための型システム

３．学会等名
電子情報通信学会ソフトウェアサイエンス研究会

４．発表年
2020年

１．発表者名
桑原 寛明, 國枝 義敏

２．発表標題
機密度パラメータ付き情報流解析のための型検査アルゴリズムとJavaアノテーション

３．学会等名
FOSE 2019

４．発表年
2019年

１．発表者名
長谷川 健太, 桑原 寛明, 國枝 義敏

２．発表標題
Java Stream API によるストリーム操作の停止性検査のための型システム

３．学会等名
FOSE 2018

４．発表年
2018年

１．発表者名
桑原 寛明, 國枝 義敏

２．発表標題
情報流解析における制約付き機密度パラメータ

３．学会等名
FOSE 2018

４．発表年
2018年

１．発表者名
長谷川 健太，吉田 真也，桑原 寛明，上原 哲太郎，國枝 義敏

２．発表標題
JavaのStream APIによるストリーム操作の停止性を検査する型システム

３．学会等名
PPL 2018

４．発表年
2018年

１．発表者名
荒木 良仁，桑原 寛明，國枝 義敏

２．発表標題
Stream APIを利用するJavaプログラムにおけるストリーム再利用の静的検出手法

３．学会等名
情報処理学会ソフトウェア工学研究会

４．発表年
2019年

１．発表者名
吉田 真也，桑原 寛明，國枝 義敏

２．発表標題
オブジェクト指向言語の情報流解析における機密度のパラメータ化

３．学会等名
FOSE 2017

４．発表年
2017年

１．発表者名
長谷川 健太，吉田 真也，桑原 寛明，上原 哲太郎，國枝 義敏

２．発表標題
Java Stream API によるストリーム操作の停止性検査のための型システム

３．学会等名
FOSE 2017

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関