様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月６日現在

機関番号：14603
研究種目：基盤研究（C）一般
研究期間：2008～2010
課題番号：20500034
研究課題名（和文）　言語組込みアクセス制御の高信頼化に関する研究

研究課題名（英文）　Automatic Analysis and Generation Methods for Language-based Access Control

研究代表者
関　浩之（SEKI HIROYUKI）
奈良先端科学技術大学院大学・情報科学研究科・教授
研究者番号：80196948

研究成果の概要（和文）：本研究ではまず，再帰プログラムPとセキュリティ仕様Sが与えられたとき，Sを満たすようにPにアクセス権検査文を埋め込む自動生成問題を定義した．そして，自動生成問題がco-NP困難であることを示した．次に，プッシュダウンシステム(PDS)モデル検査法を利用して自動生成問題を解くアルゴリズムを提案した．さらに提案アルゴリズムに基づく自動生成ツールを実装し，いくつかの例題について現実的な時間でアクセス権検査文の埋め込みが行えることを実証した．

研究成果の概要（英文）：We defined the automatic generation problem as the one to insert access check commands into a given recursive program so that the program satisfies a given security specification. First, the problem was shown to be co NP-hard. Next, we proposed an algorithm solving the automatic generation problem based on PDS model checking. We also showed that the proposed algorithm works efficiently for sample programs based on the experiments conducted on the automatic generation tool.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,400,000	420,000	1,820,000
2009 年度	1,000,000	300,000	1,300,000
2010 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：計算機科学
科研費の分科・細目：情報学・ソフトウェア
キーワード：アクセス制御，情報流解析，セキュリティ，実行履歴，スタック検査，自動生成，静的解析

１．研究開始当初の背景

コンピュータネットワークの普及により，家庭など日常的なコンピュータの利用においても，ユーザのプライバシ保護やシステムのセキュリティ保全が重要な課題となっている．例えば，インターネット経由でプログラムをダウンロードして実行するアプリケーションが増加している．しかし，悪意あるサイトからダウンロードされたプログラムがユーザのパソコン内の個人情報を窃盗したり破壊したりするといった攻撃を行う可能性がある．このような脅威からユーザとシステムを保護するため，十分なアクセス制御機構を導入する必要がある．具体的に，アクセス制御機能をプログラム言語の実行時ライブラリとして提供し，プログラムの任意の実行点からアクセス制御ライブラリを呼び出して動的にアクセス権の検査が行える仕組みが実現されている．

これを，言語組込みアクセス制御(language-based access control) とよぶ．JVM (Java Virtual Machine)等で提供されているスタック検査はこの典型的な実現例である．しかしプログラムのどの実行点でアクセス権検査を行うかはその作成者に委ねられており，必要十分なアクセス権検査がプログラム内に配置されていることを人手で確認することは困難である．我々はこの問題を解決するため，既存のいくつかの言語組込みアクセス制御機構を取り上げ，そのモデル検査法を考察してきた．そして実際にモデル検査ツールを実装し，オンラインバンキングシステムなどの例題について，提案手法がプログラムの安全性検証に有効であること，および，検証アルゴリズムの最適化により検証自身の効率を向上できることを実証してきた．

２．研究の目的

我々の従来研究は，人手で挿入したアクセス権検査文が意図（仕様）通りに機能するかの自動検証を実現したものであるが，与えられた仕様を満たすようアクセス権検査文自体を自動的に挿入できればさらに望ましい．

そこで本研究では，適切な言語組込みアクセス制御を前提とし，与えられた仕様を満たすよう，プログラムにアクセス権検査文を自動挿入するための，ソフトウェアの解析・自動生成技術を開発することを目的とする．

３．研究の方法

(1) 問題の定義：自動生成問題を形式的に定義するため，アクセス制御モデルとしてAbadiとFournetの提案した実行履歴に基づくアクセス制御 (history-based access control, HBAC)を用い，セキュリティ仕様は情報流の概念に基づいて与えることとする．

(2) 問題の難しさの理論的評価：計算量的複雑さの理論を用い，(1)で定義した自動生成問題の難しさを見積もる．

(3) アルゴリズムの提案：(2)と並行し，自動生成問題を解くアルゴリズムを考案する．我々は既にプッシュダウンシステム(PDS)に基づくモデル検査法を応用し，HBACのアクセス検査文を含む再帰プログラム（HBACプログラムと略記）の自動検証法を提案している．そこで，この自動検証法を利用して，まず与えられたプログラムを静的に解析する．その結果，仕様を満たさない実行が起こりうるとわかった場合，そのような実行を強制終了させるよう，アクセス権検査文を挿入するという方針をとる．

(4) 提案手法の評価：(3)で開発したアルゴリズムを実装し，例プログラムを用いて提案手法の有効性の評価を行う．

４．研究成果

(1) アクセス制御モデルとして３節で述べたHBACを仮定し，セキュリティ仕様は情報流の概念を用いて与えることとした．

（**HBACプログラム**）通常の再帰プログラムにおいて，以下の拡張を行ったものPを，HBACプログラムという．

①Pはメソッドの有限集合とアクセス権の有限集合の2項組 P = (Mthds, Prms) であり，Pの各メソッドmにはアクセス権の部分集合 SP(m)（⊆Prms）が割当てられる．これをmの静的アクセス権集合とよぶ．

②プログラムは任意の位置に，check(Q)という形式のアクセス権検査文(check文)を含んでよい．ここでQはPrmsの部分集合であり，このcheck文のパラメータとよばれる．

Pの各実行状態には動的アクセス権集合が割当てられる．本研究では，HBACのもっとも単純な場合であるshallow HBACを用いるが，この場合，Pの実行時アクセス権集合Dは以下のように定義される．

①実行開始時，動的アクセス権集合はメインメソッドm_0の静的アクセス権集合$SP(m_0)$に初期化される．

②動的アクセス権集合がDであるときにメソッドmが呼ばれると，動的アクセス権集合は$D \wedge SP(m)$に更新される．

③動的アクセス権集合がDのときにcheck(Q)が実行されると，$Q \subseteq D$のとき，すなわち，check文のパラメータに指定されているアクセス権が動的アクセス権集合にすべて含まれているとき実行は継続され，そうでないとき，アクセス制御違反が発生したとして実行は強制的に中断される．

通常，check文はプログラムにおいて機密度の高いデータに直接アクセスを行う直前に配置すればよいので，check文の配置自体はそれほど困難ではない．一方，各メソッドにどのようにアクセス権を静的に割当て，各check文のパラメータをどのように設定すべきかを決定するのは困難な問題である．

そこで本研究ではこのパラメータを自動設定する手法を開発するが，そのための基準としてセキュリティ仕様（情報流仕様）を以下のように定義する．

（**情報流仕様**）プログラムPに対する情報流仕様（あるいは単に仕様）Sとは，Pに現れるプログラム変数への機密度の割当てである．ここで機密度とは，topsecret, confidential, normalのように，データがどの程度の機密度をもつのかを表すラベルである．本研究では簡単

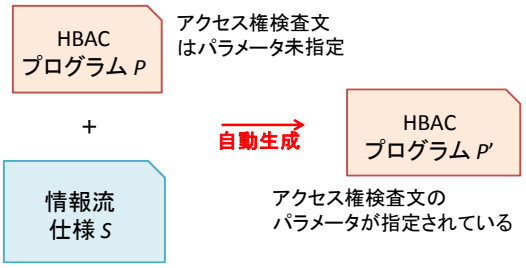
のため，機密度として，H(High), L(Low)のみを仮定する．

プログラムPが仕様Sに関して非干渉性(noninterference)をもつとは，「機密度がHである入力変数の値が変化しても，機密度がLである出力変数の値が変化しない」ことをいう．

本研究のターゲットは（図1参照），アクセス権検査文のパラメータが指定されていないHBACプログラムPと情報流仕様Sが与えられたとき，次の条件を満たすHBACプログラムP'を生成することである：

①P' はSに関して非干渉性を満たす．
②P' 現れるアクセス権検査文のパラメータは指定されている．
③同一の入力に対して，もしPとP'がともに停止するならば，それらの出力は一致する．

図1　本研究のターゲット



非干渉性はプログラムが機密性を保持する（漏洩しない）ことを表す自然な概念である．しかし，非干渉性は一般の再帰プログラムに対しては決定不能であることが知られている．

そこで本研究ではまず，HBACプログラムPとセキュリティ仕様Sに対し，Sにおける機密度を型とみなすことでSの下でのPの型安全性を定義した．そして，PがSの下で型安全ならば，PはSに関して非干渉性を満たすこと（型安全性は非干渉性の十分条件であること）を証明した．

(2) 自動生成問題を「再帰プログラムPとセキュリティ仕様Sが与えられたとき，PがSの下で型安全となるようPにアクセス権検査文を挿入する問題」と定義し，自動生成問題がco-NP困難であることを証明した．証明は3SATの補問題（与えられた3CNFが充足不能かどうかの判定問題）からの帰着により行った．

(3) プッシュダウンシステム(PDS)のモデル検査法を利用して自動生成問題を解くアルゴリズムを提案した．PDSは再帰プログラムスキームの簡潔な計算モデルである．提案アルゴリズムは次の２つのステップからなる．

(ステップ1) 与えられたプログラムPにおいて変数値をその機密度（型）に抽象化することによりPをPDS Mに変換する．Pにおける大域的状態を(n, μ, D)，ここでnはプログラム中の実行点，μは変数への値の割当て，Dは動的アクセス権集合，とするとき，これを，(n, sc, D)に抽象化する．ここで，scは変数への機密度の割当てである．

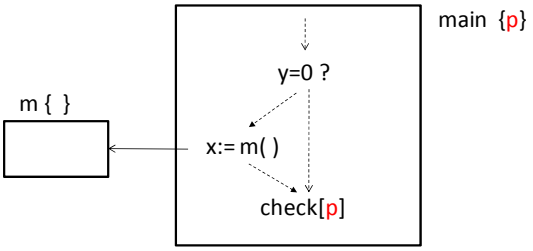
(ステップ2) Mに対してモデル検査を実行し，もし型安全性に反する実行が発見されれば，その実行が強制終了されるようMにアクセス権検査文を挿入する．

紙面の都合でここでは自動生成アルゴリズムの詳細は述べないが，本研究において特に工夫した点について，以下で直観的に述べる．

①PDSモデル検査によって，型安全でない（したがって仕様Sを満たさない可能性のある）実行を検知した際，それを強制終了できるための情報を得るため，上記(ステップ1)のPDSの状態を，(n, sc, D, (n', Q'))と拡張する．ここで，n'はモデル検査において通過したcheck文，Q'はn'において実行を強制終了できるアクセス権の部分集合（n'のパラメータ）である．

②動的アクセス権検査自体が情報漏洩の原因となることがある．例えば図2のプログラムにおいて，SP(main)={p}, SP(m)={ }であるため，mを呼び出すと動的アクセス権集合は空集合となる．よって，check[p]において実行が強制終了するかどうかを外部から観察すれば，y=0であるかどうかを知られてしまう．一般に，あるcheck文にパラメータとしてアクセス権を追加すると，その副作用により，あらたに非干渉性を満たさない実行が生じる可能性がある．アルゴリズムの(ステップ1)で，上記のような現象も反映した不動点計算による解析を行い，副作用による情報漏洩が発生しないことを保証している．

図2　アクセス権検査による情報漏洩例



(4) 提案手法に基づいて自動生成システムを実装し，いくつかの例題に対して実験を行った結果，実用的な時間で自動生成が行えることを実証した．具体的に，「互いにセキュリティレベルの異なるk個の入力変数から一つを非決定的に選択して内部変数にその値を代入し，次に，互いにセキュリティレベルの異なるk個の出力変数のいずれか一つにその内部変数の値を書き出す」というプログラム$\pi_a(k)$および，$\pi_a(k)$を任意の回数繰り返すプログラム$\pi_b(k)$をベンチマークとして自動生成実験を行った．その結果，自動生成の前段で行うPDSモデル検査において探索された到達可能状態数は図3のようになった．また自動生成に要した時間は図4 の通りであった．図4 より，例えば$\pi_a(k)$については，k=200でも20秒以内で自動生成が可能であることを実証した．

図 3　PDSの到達可能状態数

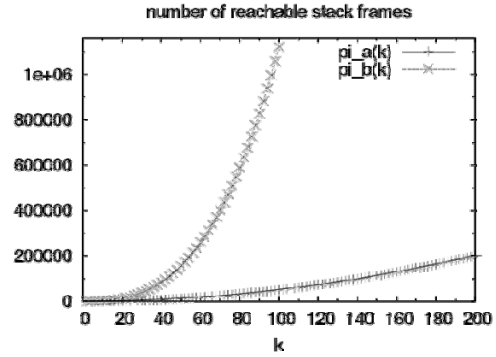
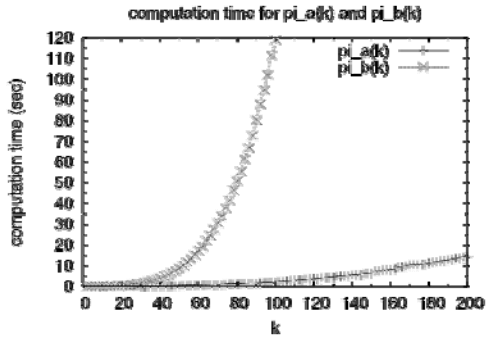


図 4　自動生成に要した計算時間



(5)　関連するテーマとして，言語組込みアクセス制御に分類されるいくつかのモデルの表現能力の比較を行った．その結果，AbadiとFournetらによる実行履歴に基づくアクセス制御(HBAC)，正則パターンに基づくスタック検査(R-SI)，Fongの狭履歴オートマトンの３つの形式モデルについて，そのどの２つの組合せを考えても一方が他方よりも表現能力が大きくないことを証明した．またHBACを拡張し，R-SIより表現能力が大きいモデルを提案した．

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２件）

① Yoshiaki Takata and Hiroyuki Seki, Comparison of the expressive power of language-based access control models, IEICE Transactions on Information and Systems, E92-D(5), 1033-1036, 2009. 査読有.

② Yoshiaki Takata and Hiroyuki Seki, Formal language theoretic approach to the disclosure tree strategy in trust management, IEICE Transactions on Information and Systems, E92-D(2), 200-210, 2009. 査読有.

〔学会発表〕（計１５件）

① Yoshiaki Takata and Hiroyuki Seki, Automatic generation of history-based access control from information flow specification, 8th International Symposium on Automated Technology for Verification and Analysis, 2010.9.23, Singapore, Lecture Notes in Computer Science 6252, 259-275, 査読有.

② 高田喜朗，関浩之，森田剛正，情報流仕様に基づくアクセス権検査文自動生成法，日本ソフトウェア科学会第 12 回プログラミングおよびプログラミング言語ワークショップ論文集，161-175, 2010.3.4, 香川県多度郡琴平町，査読有.

③ 関浩之，ソフトウェアの静的解析と動的検査　－言語ベースセキュリティを例にして－，情報処理学会組込みシステムシンポジウム 2009，2009.10.21，東京，招待講演.

④　森田剛正，高田喜朗，関浩之，情報流解析に基づくアクセス制御文の自動生成，電子情報通信学会ソフトウェアサイエンス研究会，電子情報通信学会技術研究報告 SS2009-23, 2009.8.7, 北海道北見市. 査読無.

⑤　高田喜朗，森田剛正，関浩之，情報流解析に基づくアクセス権検査文自動挿入法，日本ソフトウェア科学会第 7 回ディペンダブルワークショップ論文集，99-103，2009.7.15, 北海道亀田郡七飯町，査読無.

⑥　関浩之，アクセス制御　－言語ベースセキュリティをめざして－，日本ソフトウェア科学会第 7 回ディペンダブルワークショップ論文集, 93-98, 2009.7.15，北海道亀田郡七飯

町，招待講演.
⑦ 高田喜朗，関浩之，情報流からの言語組み込みアクセス制御文の挿入，日本ソフトウェア科学会第６回ディペンダブルワークショップ論文集, 141-143, 2008.7.4, 函館, 査読無.

６．研究組織
(1)研究代表者
関　浩之（SEKI HIROYUKI）
奈良先端科学技術大学院大学・情報科学研究科・教授
研究者番号：80196948

(2)研究分担者：なし

(3)連携研究者
高田　喜朗（TAKATA YOSHIAKI）
高知工科大学・工学部・准教授
研究者番号：60294279