論 文 内 容 の 要 旨

博士論文題目

Security Assurance Methods for Access Control Systems
Using Static Analysis

氏　名　國信　茂太

（論文内容の要旨）

計算機システムセキュリティ保全の基盤技術として、暗号とともにアクセス制御法が古くから研究されている。アクセス制御法は、必須アクセス制御 (Mandatory Access Control, MAC)と任意アクセス制御(Discretionary Access Control, DAC)に大別される。MAC はシステム全体で設定したセキュリティレベル (topsecret, secret, unclassified 等)をデータ、ユーザの双方に割当て、これに基づいてアクセス許可／禁止を決定する。DAC では、例えば UNIX のファイルパーミッションのようにデータごとに所有者がアクセスポリシーを設定できる。

本論文では、MAC および DAC の両モデルについて、設定されたアクセス制御ポリシーによって、システム全体に対するセキュリティ要求が達成されているかを、ソフトウェアの静的解析を用いて判定する方法が提案されている。

2 章では、MAC に対するセキュリティ保全手法として、手続き型プログラムに対する情報フロー解析アルゴリズムが提案されている。提案アルゴリズムは、解析対象プログラムとそのプログラムへの入力データのセキュリティレベルが与えられたとき、出力データのセキュリティレベルを推論する。提案手法では、セキュリティレベルの構造は任意の有限束で表現することができる。解析手法として、抽象解釈(abstract interpretation)法を用いることにより、任意の再帰プログラムに対する解析を可能としている。解析法の健全性の証明が与えられており、提案アルゴリズムの時間計算量がプログラムサイズの 3 乗オーダで実行できることも示されている。さらに、暗号化関数等、入力情報を隠蔽する機能を組込み演算としてもつプログラムの解析を目的として提案アルゴリズムを拡張する方法も述べられている。試作システムを用いて、例プログラムを解析した結果についても議論されている。

3 章では、DAC に基づいたシステムのセキュリティ保全手法が提案されている。まず、簡潔なポリシー記述言語が提案され、その構文と意味が定義されている。従来の DAC モデルでは、ポリシーとしてアクセス許可およびアクセス禁止の 2 種類を記述することができるが、提案するポリシー記述言語では、義務ポリシーも記述することができる。義務ポリシーとは、あるイベントが発生したときに義務的に実行されなければならない動作を記述するポリシーである。ポリシー制

御系(Policy Controlled System, PCS)とは、個々のオブジェクトがそれぞれにセキュリティポリシーをもち、オブジェクトのふるまいをポリシーにより制御するようなシステムである。次に、「PCS Pと検証条件Fが与えられたとき、Pの到達可能な状態は全てFを満たすか」という安全性検証問題を設定し、プッシュダウンシステムに対するモデル検査法を用いた検証法が提案されている。最後に、試作システムを用いて例PCSの検証を行った結果が示されている。

氏 名	國信 茂太

（論文審査結果の要旨）

近年、コンピュータネットワークの普及により、不正な攻撃者に対する計算機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。セキュリティ保全の基本的な技術として、暗号とともにアクセス制御法が古くから研究されている。アクセス制御法は、必須アクセス制御(Mandatory Access Control, MAC)と任意アクセス制御(Discretionary Access Control, DAC)に大別される。MACでは、セキュリティレベル(top-secret, secret, unclassified等)が各ユーザおよび各データにセキュリティポリシーとして割り振られており、アクセス制御はユーザのセキュリティレベルとそのユーザがアクセスしようとするデータのセキュリティレベルを比較することにより実行される。DACでは、各データの所有者がそのデータに対し、自由にセキュリティポリシー(アクセス条件)を設定することができ、アクセス制御はアクセスされるデータのセキュリティポリシーに基づいて実行される。UNIXのファイルパーミッションはDACの典型的な例である。しかしながら、DAC/MACのどちらのアクセス制御法においても、与えられたセキュリティポリシーによりシステム全体の本来満たすべき目的が達成されているかを人手で確認することは難しい。

本論文では、MAC, DACの両モデルについてそれぞれ、システム管理者あるいはデータ所有者が設定したアクセス制御のポリシーによって、所期のセキュリティ要求が達成されているかどうかを、それぞれ、抽象解釈法とモデル検査法と呼ばれる静的解析法によって判定する方法を提案している。

まず、MACについて、「有限束で表現されたセキュリティレベルとプログラムPが与えられたとき、Pへどのようなセキュリティレベルのデータを入力すると、出力にはどのようなセキュリティレベルのデータが現われ得るか」を解析する、いわゆる情報フロー解析法（データフロー解析法の一種）が提案されている。 解析手法として抽象解釈法を用いることにより、任意の再帰プログラムに対する解析を可能としている。さらに、本手法に基づいて実装された解析系を用いて行った実験結果についても報告されている。また、暗号化関数や集計関数（平均値計算等）のように、入力情報を隠蔽する効果をもつ組込み演算を含むプログラムの解析を目的として、解析法の拡張が行われている。

次に、DACについて、システム管理者がセキュリティポリシーを記述するための言語（ポリシー記述言語と呼ぶ）が定義されている。このポリシー記述言語では、従来のアクセス許可／禁止ポリシーに加えて、義務実行を規定する義務ポリシーを記述することができる。この言語で記述されたポリシーに基づきプログラムの実行制御を行う系をポリシー制御系（Policy Controlled System, PCS）と呼ぶ。「PCS Pと性質Fが与えられたとき、Pで到達可能な状態がすべてFを満

すか」という問題を安全性検証問題と呼ぶ。これは広義のコントロールフロー解析問題の一種ともいえる。 検証問題にはこのタイプの他、生存性（活性）検証問題等も考えられるが、セキュリティ保全に関する検証には安全性問題で十分と考えられる。本論文では、PDS（プッシュダウンシステム，Pushdown System）に対するモデル検査法を用いることにより、この安全性検証問題を解く手法が提案されている。また、試作した自動検証系を用いた検証例が述べられ、本手法の有効性が明らかにされている。 義務ポリシーは、最近注目されているアスペクト指向プログラミング、アクティブデータベース等とも関連があり、本研究を契機とし、これらの計算モデルに基づく検証法への展開も期待される。

以上の通り、本論文で提案する手法と得られた結果は、情報セキュリティ、とりわけアクセス制御技術の開発と運用の高信頼化に関する重要な知見を与えており、博士（工学）の学位論文として価値あるものと認める。