論 文 内 容 の 要 旨

博士論文題目　Efficient Access Control and Detection of Security Flaws under Authorizations in Object-Oriented Databases
(オブジェクト指向データベースにおけるアクセス権の下での効率のよいアクセス制御法およびセキュリティフロー検出に関する研究)

氏　名　森多俊之

(論文内容の要旨)

データベース管理システム (DBMS) においてアクセス制御はデータ保護のための重要な技術である. アクセス制御を実現する方法として様々なアクセス権モデルが提案されている. 一般に, アクセス権は「誰がどのデータに対してどのような操作を実行できるか」を表す組の集合として記述される. 本論文では, 特定のオブジェクト指向データベース (OODB) スキーマとアクセス権管理方針に依存しない OODB に対するアクセス権モデルを提案し, アクセス権を記述するために実用上十分な能力をもつアクセス権記述言語を定義する. また, 本論文で定義したアクセス権記述言語により記述されたアクセス権の下で, アクセス制御を効率的に実現する方法を提案する.

一方, DBMS がアクセス権を用いてアクセス制御を実施していたとしても, セキュリティフローが起こる可能性がある. セキュリティフローとは「データベース利用者がアクセス権の下で許可された情報のみを用いて, アクセス権で禁止された情報を得る」ことである. 本論文では, OODB におけるセキュリティフローを検出する以下の問題を議論する:

(1) OODB インスタンスに対するセキュリティフロー検出問題: データベーススキーマ S, データベースインスタンス I, アクセス権 A, 機密情報を取り出す質問プログラム τ が与えられたとき, 利用者は S, I, A の下で τ の実行結果を推論することができるか.

(2) OODB スキーマに対するセキュリティフロー検出問題: データベーススキーマ S, アクセス権 A, 機密情報を取り出す質問プログラム τ が与えられたとき, 利用者が S, I, A の下で τ の実行結果を推論することができるようなデータベースインスタンス I が存在するか.

まず, 問題 (1) は実用的な場合に多項式時間可解であることを示す. 次に, 問題 (2) は決定不能であることを示し, τ に関してセキュリティフローが起こらないための決定可能な十分条件を提案する. また, 与えられたデータベーススキーマがモナディック (つまり, すべてのメソッドが 1 引数) であるなら, 前述の十分条件は必要条件でもあることを示す. さらに, この十分条件を決定するアルゴリズムを提案し, アルゴリズムの計算量を評価する.

氏 名	森多俊之

(論文審査結果の要旨)

近年のデータベースセキュリティ技術の発達に伴い, データベースへの不正アクセス防止を実現するために, これまで様々なデータベースへのアクセス制御法が提案されている. また, 機密情報の漏洩防止を実現するために, セキュリティフローの可能性を検出する研究もおこなわれている. 本論文は, オブジェクト指向データベース (OODB) においてアクセス制御を実現するアクセス権モデルを提案し, アクセス要求を効率的に判定する方法を示している. さらに, セキュリティフローを形式的に定義し, セキュリティフローの可能性を検出する問題を考察している. 本論文の主な成果は次のように要約される.

(1) 特定の OODB スキーマとアクセス権管理方針に依存しない OODB に対するアクセス権モデルを提案している. また, アクセス権を記述するために実用上十分な能力をもつ汎用的かつ柔軟なアクセス権記述言語を定義している. さらに, アクセス権記述言語により記述されたアクセス権の下で, アクセス制御を効率的に実現する方法を提案し, シミュレーションをおこなうことによりその効率性を検証している.

(2) セキュリティフローを検出するために, データベースユーザがアクセス権の下で得られる情報を形式的に定義している. そして, OODB におけるセキュリティフローを検出する次の二つの問題, (a) OODB インスタンスに対するセキュリティフロー検出問題, および (b) OODB スキーマに対するセキュリティフロー検出問題を考察している. まず, 問題 (a) は実用的な場合に多項式時間可解であることを示している. 次に, 問題 (b) は決定不能であることを示し, セキュリティフローが起こらないための決定可能な十分条件を提案している. また, モナディックスキーマに対しては, 前述の十分条件は必要条件でもあることを示すことにより, モナディックスキーマに対する問題 (b) は決定可能であることを示している. さらに, この十分条件を決定するアルゴリズムを提案し, アルゴリズムの計算量を評価している.

以上のように, 本論文は, データベースのアクセス制御を効率的に実現する手法を提案するとともに, セキュリティフローの可能性を検出する問題を考察することにより, セキュリティフロー検出の有用性を示したものである. データベースセキュリティの分野において, 学術上, 実用上寄与するところが多い. よって, 本論文は博士 (工学) の学位論文として充分に価値のあるものと認める.