論文の内容の要旨

論文題目　Algebraic and Logic-based Authorization Models for Provisional Access Control
（和訳　必須処理付きアクセス制御の代数型および論理型モデルに関する研究）

氏　名　工藤　道治

本研究は、理論面 / 実用面の両面において先に述べたセキュリティポリシーのための統合的な枠組みを提供することを目的として、従来のアクセス制御モデルに新しく必須処理という概念を組み込むことを提案する。必須処理とは、情報資源に対するアクセスを認可する際の前提条件を表現する概念である。これにより、インターネット上のシステムで執行される多様なセキュリティポリシーを、アクセス制御モデルの下で統一的に表現し、かつそれをシステムが執行することを可能にする。本研究で得られたセキュリティポリシー構成モデルは、従来のアクセス制御モデルでは表現できなかった幅広い範囲のセキュリティポリシーを、実用化の観点から十分高速に実行できることが特長である。本学位論文は以下に示すように全部で七つの章から構成される。

第１章では、コンピューターセキュリティにおける中心的な研究課題の一つであるアクセス制御問題について一般的に述べる。本論文では、従来のアクセス制御モデルに新しく「必須処理」という概念を導入するが、このような拡張モデルが従来の提案モデルに対してどのように位置付けられるかを言及すると共に、関連研究についても説明する。

第２章では、本論文で扱う拡張モデル、必須処理付きアクセス制御モデルの基本構成について説明する。提案モデルの基本構成は、従来の三つ組み(主体、客体、権限)によって表現されるアクセス制御規則に対し、「必須処理」という四番目のパラメータを追加する。これにより、ある客体はある主体に対してある権限を実行してよい、ただし認可の前提条件として指定された必須処理を実行しなければならない、というポリシーを記述することができる。このようなポリシー表現により、データシステム全体が満たすべき整合性という性質と、データの持つべき秘匿性という性質の両方を一つのモデルの下で統合して表現できるという利点があることを示す。また、提案アーキテクチャは、実システムへの適用が容易であるという利点を持つことも示す。

第３章では、必須処理付きアクセス制御モデルの具体的な構成方法として、論理表現に基づくモデル化を行う。この論理モデルは、汎用性を目指した論理型認可モデルとしてよく知られているASL 言語の拡張言語として位置付けられる。本提案モデルは、階層的な客体や主体の構造、必須処理、アクセス制御規則、伝播規則等、アクセス制御に関係する全ての要素を論理式として表現する。アクセス制御規則を表現する述語の構文とセマンティクスを拡張し、述語に必須処理の

概念を付加した。本論文では、論理式の具現化を行うマテリアライゼーションという手法を用いて本提案モデルを実装した。計算機実験では、実用的なデータサイズに対して十分高速にアルゴリズムが動作することを示す。

第４章では、必須処理付きアクセス制御モデルの第二の具体的な構成方法として、代数表現に基づくモデル化を提案する。この代数モデルは、商用で使われている必須処理を持たないアクセス制御システムの理論モデルとしても機能するという特長がある。提案モデルは次のように構成される。まず代数モデルの中で複数の客体や主体を階層的に表現する木を定義する。次に複数の木の要素同士の関係として必須処理付きアクセス制御規則を定義する。最後に、前述の構成要素によって表現されたアクセス制御規則に基づいてアクセス判定を行うアルゴリズムを定義する。本代数モデルは機能別の二つの階層から構成されており、低層の構成要素である基礎モデルと、基礎モデル上で定義される通常の認可モデルおよび必須処理認可モデルによって構成される。本提案モデルに基づいた計算機実験を行い、実用的なデータサイズに対して非常に高速にアルゴリズムが動作することを示す。

第５章では、第３章と第４章で提案した二つの構成モデルの表現能力と計算機実験の比較解析を行う。必須処理のないポリシーの表現能力に関しては、階層的に構成された客体や主体に対する伝播機能と矛盾解消機能を中心とした詳細な評価を行う。必須処理付きのポリシーの表現能力に関しては、代数モデルと論理モデルがそれぞれ異なる方針に基づいて必須処理を計算していることを示す。両者のモデルが持つ一般的な性質として、アクセス制御ポリシーの記述に対する完全性と安全性について考察する。最後に、両モデルの計算機実験の結果を比較する。

第６章では、必須処理付きアクセス制御モデルが、非常に広い範囲のセキュリティポリシーを表現できることを示す。実際のネットワーク構成にならい、クライアントマシン、ファイアーウォールサーバ、セキュリティサーバ、データサーバ、アプリケーションサーバの五つの構成要素に分類し、各々に対して網羅的にセキュリティポリシーを記述することにより提案モデルの表現能力の高さを示す。従来のアクセス制御モデルでは実現できないが、本提案モデルによって実現できる有用なアプリケーションの具体例として、ユーザのプライバシーを守るためのプライバシーポリシー、デジタルデータに対するユーザ権限を表すデジタル権限ポリシー、サービスに対する課金のポリシー、機密データに対するポリシー、データのインテグリティを保証するポリシーなどが挙げられる。

第７章では、本論文の結果をまとめる。必須処理付きアクセス制御モデルは、従来のアクセス制御モデルでは記述できなかった実用的で非常に幅の広いセキュリティポリシーを記述することのできるモデルである。論理型モデルは、セキュリティポリシーの記述力において、伝播ポリシーの表現能力、条件記述、およびインテグリティルールの記述において代数型モデルより優れている。代数型モデルは、ポリシー評価の実行速度、基本構成の単純さの点において論理型モデルよりも優れている。両モデルはアクセス判定の評価速度の点において、データ量が多く（３０００ユーザ以上）、アクセス制御規則の数が多い場合（２０００以上）においても、実用上問題のない高速な評価（０．３ミリ秒以下）が可能であることを示した。