審査の結果の要旨

論文提出者氏名　　工藤　道治

本論文は「Algebraic and Logic-based Authorization Models for Provisional Access Control（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）」と題し，情報セキュリティポリシーの記述と執行の統合的な枠組みを提供することを目的として，必須処理という新しい概念を組み込んだアクセス制御手法を提案している．提案手法に対して論理型モデルと代数型モデルによる2種類の定式化を行い，①セキュリティポリシーの記述力，②セキュリティポリシーの効率的な執行方式，③実システムにおける適用可能性，の三つの観点から検討している．幅広いセキュリティポリシーをできるだけシンプルなモデルで表現することが求められる一方，いかに効率よく高速にセキュリティポリシーを評価するかも実用上重要である．本論文は，これらの問題に対し，有効な解決策を示したものであり，7章からなる．

第1章は「Introduction（序論）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第2章は「Provisional Authorization Model（必須処理付き認可モデル）」と題し，本論文で扱う必須処理付き認可モデルの基本構成を示している．従来の三つ組(主体，客体，権限)によって表現されるアクセス制御規則を拡張し「必須処理」という第4のパラメータを追加することで，「ある客体はある主体に対してある権限を実行できるが，そ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」というセキュリティポリシーを表現できる．これにより，システム全体が満たすべき整合性と守秘性を，必須処理付き認可モデルの下で統合的に表現できる．

第3章は「Logic-based Authorization Model（論理型認可モデル）」と題し，論理モデルに基づいて必須処理付き認可モデルの定式化を行っている．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ことが特徴である．本論文では，論理式の集合に対する問い合わせを高速に実行するために，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提案し，計算機実験により，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している．

第4章は「Algebraic Authorization Model（代数型認可モデル）」と題し，代数モデルに基づく必須処理付き認可モデルの定式化を行っている．まず複数の客体や主体を表現する木を定義し，次に複数の木にまたがる要素同士の関係としてアクセス制御規則要素を定義する．そしてアクセス制御規則要素と階層構造，階層伝播，矛盾解消パラメータに基づいて高速にアクセス判定を行うアルゴリズ

ムを定義し，計算量の評価を行っている．さらに、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している．

第5章は「Model Analysis（モデル解析）」と題し，第3，4章で提案した二つの構成モデルにおけるセキュリティポリシーの表現能力，実行速度，安全性，意味モデルなどに関する比較検討を行っている．論理型モデルの方が優れている項目として，セキュリティポリシーにおけるユーザモデルをより的確に表現できること，セキュリティポリシーや階層データの記述の不整合を検出できること，サポートしている伝播機能や矛盾解消機能の種類が多いこと，などが示されている．逆に代数型モデルの方が優れている項目として，実行速度が客体や主体の数に依存しないこと，非常に高速にアクセス判定を実行できること，単純なシステム構成で実現できること，などが示されている．

第6章は「Policy Specification Examples（セキュリティポリシー記述例）」と題し，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実例により示している．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応用の具体例として，ユーザのプライバシー保護の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，Web サービスにおけるサービスポリシー，機密性や完全性を必要とするデータに対するポリシーなどが示されており，本提案方式の広い適用可能性を示している．

最後に第7章は「Conclusion（結言）」で，本研究の総括を行い，併せて将来展望について述べている．

以上これを要するに，本論文は，必須処理付きアクセス制御に関する基礎検討を行うとともに，情報セキュリティポリシーの表現，執行およびその応用に対する具体的な手法を明示したものであり，電子情報工学上貢献するところが少なくない．

よって本論文は博士（工学）の学位請求論文として合格と認められる．