博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　ステートフル・アクセス制御システムの研究
申請者　：　橋本正樹
審査委員会　：　主査　教授　田中英彦
副査　教授　板倉征男
副査　教授　小柳和子
副査　教授　松尾和人
副査　客員准教授　辻秀典

Ⅰ．論文内容の要旨

本論文は、「ステートフル・アクセス制御システムの研究」と題し、7 章と付録などからなる。情報システムは社会基盤として重要な役割を果たしているが、インターネットなどの普及により情報システムに対する脅威が飛躍的に増大しているにも関わらず、セキュリティ確保のコアとなるべきセキュア OS は使いやすさなどで問題があり広く使われる状況には至っていない。この研究は、そのような状況を打開すべく、必要十分な粒度で認可判定を可能とする見通しよい認可ポリシー記述言語の提案と、それをシステム内に組み込む手法について考察したものである。

第１章は「序論」で、本研究の背景と研究の目的、特徴及び論文の構成についてまとめたものである。

第２章は「研究の背景」で、現在の情報システムのセキュリティ確保のために情報システム内で用いられている方式を概観し、それが各アプリケーション内で閉じたセキュリティ確保になっており OS のアクセス制御機能を十分生かし切れていないことを述べるとともに、代表的な従来のセキュア OS 機構についてまとめ、その限界について考察している。すなわち、それらは、単一システムをベースとした OS になっていること、アクセス制御の粒度が余りにも細粒度であるために全体としてのアクセス制御の見通しに欠けることなどで、それらは今後の分散処理の隆盛を考えると、大きな問題であることを指摘している。

第 3 章は「ポリシーに基づく分散アクセス制御に向けた検討」で、第 2 章の考察を踏まえ、分散処理に適合したセキュリティ基盤の要件をまとめ、それを実現するための分散システム全体に透過なアクセス制御モデルを提案している。それは、分散処理の権限管理を記述するポリシー記述法と、それを強制するためのアクセス制御機構からなり、Capability を利用したアクセス制御をおこなうモデルである。

第４章は「Capability を基礎とした分散アクセス制御機構」で、上記モデルを実現する分散アクセス制御機構について検討している。まず、Capability を用いることにより、従来のアクセス制御リスト方式に比して、制御の粒度を細かくでき、また、分散アクセスの認可問い合わせ処理をローカルシステムに閉じて実行することが可能となることを述べ、次に、ISO10181-3 のアクセス制御フレームワークに環境情報と遠隔アクセス機能を加えて拡張することにより、分散アクセス制御機構のブロック構成法を提案し、その詳細な動作を与えている。この構成により、

資源情報を一か所に集中配置する必要が無くなり、アクセス可能な資源情報のみをアクセス主体が保持することで実現が可能になることを示している。

第 5 章は「論理プログラミングを基礎とした認可ポリシー記述言語」で、現実的な OS のセキュリティ対策として多層防御を取り上げ、それがシステム内を細かく区画化することで有効性を高めているが、反面、ポリシー数の増大を招きその記述や理解が困難になるため利用に繋がらない現状に鑑み、論理プログラミングをアクセス制御記述に用いることにより、この解決を図ることを提案している。すなわち、個々のアクセス制御規則の記述とポリシー問い合わせの認可判定とを、論理プログラミングに基づいた構文規則とその意味、及び推論規則を定めることで定式化し、これを Datalog を用いて実装している。この章では更に、この提案言語を用いて代表的なアクセス制御モデルを構造的に記述する手法を示すとともに、SELinux のポリシーを実際に記述した実験システムを構成し、認可判定の妥当性と表現力の評価を行っている。その結果、実験システムの認可判定が SELinux の認可判定と現実的に一致すること、また記述量の比較では記述行数が 20 分の 1、リストページ数では 71%となることを述べ、この提案が有効であることを示している。

第 6 章は「今後の課題」で、残された検討課題をまとめている。すなわち、現在はユーザ領域で実装している提案システムを、実際のカーネル領域に移して実行速度の詳細な評価をすることと、この記述・判定システムを分散システムに適用し具体的な分散処理応用を対象としてその評価を行うことなどを挙げている。

第 7 章は「結論」である。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、情報システムのセキュリティを確保する上で根幹となるセキュア OS 構成方式を検討したもので、そのアクセス制御システムをより実用的なものとするために、論理プログラミングに基づくポリシー記述方式と、アクセス認可判定システムを提案するとともに、その言語処理系と認可判定システムを実装し、SELinux と比較することにより、具体的にその記述妥当性と表現力が優れていることを示したもので、今後の情報システムのセキュリティ向上と情報学に貢献するところ少なくない。

よって、本論文は、博士（情報学）の学位請求論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、2010 年 1 月 26 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。