

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 : プログラムの振る舞いに注目したアクセス制御に関する研究
申請者 : 原田 季栄
審査委員会 : 主査 教授 板倉 征男
副査 教授 田中 英彦
副査 教授 小柳 和子
副査 教授 原田 要之助
副査 教授 佐藤 直 (追加)

I. 論文内容の要旨

本論文は、「プログラムの振る舞いに注目したアクセス制御に関する研究」と題し、11章と付録などからなる。セキュリティには多様な意味と観点が存在するが、本研究では情報システムのノードであるコンピュータについて、それを本来の管理者が意図しない形で利用される脅威を防ぐことを目的として、OSにおけるアクセス制御機能を制限すること及び関連する課題の追求をテーマとし、プログラムの状態に応じた強制的なアクセス制御を行う新たな方式を提案する。

第1章では、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章では、本研究の背景となるOSのセキュリティ強化の必要性と強制アクセス制御の考案に至るアクセス制御の強化に関するこれまでの取組みについて述べる。強制アクセス制御の概念と必要性、SELinuxはじめ多くの強制アクセス制御の実装が採用しているラベルに基づくセキュリティの方式について説明する。

第3章では、本研究の成果である「プログラムの振る舞いに注目したアクセス制御」の基本となる概念と、それを実装するために必要な要素について述べる。前章で概観したラベルに基づくセキュリティは客体の視点から情報の隔離および漏えいの防止を主眼としたものでありその効果は高いがそれだけでは解決しない問題が存在する。本章ではラベルに基づくセキュリティを補完するものとして、主体であるプログラムの振る舞いに注目したアクセス制御について提案する。プログラムの振る舞いに注目したアクセス制御では、主体であるプログラムの実行されている状況ごとにその主体に認めるべきアクセス許可を定義する。またプログラムの振る舞いに注目したアクセス制御をLinux上に実装したTOMOYO Linuxの概要を示す。

第4章では、プログラムの振る舞いに注目したアクセスの主要な構成要素である「プログラム実行履歴に基づく自動ドメイン定義」と「パラメータに基づくアクセス制御」について、TOMOYO Linuxにおける実装を参考としながら説明する。プログラムの実行履歴はその定義によりプログラム名と結合して表現されるが、その一部と全体を区別するために基点となる文字列を導入する。プログラムの実行履歴の自動定義により実行されるすべてのプロセスについてそのプログラム実行履歴を持たせることが可能となる。この結果、プロセスについて一意に定められること、処理の複雑さの影響を受けないこと、子のプログラム実行履歴は親のプログラム実行履歴より求めることができ、同一のプログラムについてもその実行履歴により区別することができる。これにより単なる識別子ではなく、人間(管理者)にとって意味を持つこと、実行されたプログラムのファイル名により実行履歴を指定できるなどの特徴を備えることができる。その結果、運用についても使い易さが向上する。

第 5 章では、「パラメータに基づくアクセス制御」について述べる。プログラム実行履歴に基づく自動ドメイン定義によりプログラムについてその実行履歴に基づき分類された状態でアクセス制御を行うことが可能となるが、本章ではプログラムの振る舞いに影響を与える要因について例を挙げて示す。

第 6 章及び第 7 章では、TOMOYO Linux におけるプログラムの振る舞いに注目したアクセス制御について、それぞれ仕様と実装上の面から説明する。

第 8 章では、プログラムの振る舞いに注目したアクセス制御の応用例を示す。

第 9 章では、それまでの内容について振り返り、本研究の意義と残された課題などについて整理する。

第 10 章では、本研究に関連する他の研究について、その概要を紹介する。

第 11 章では、本研究の結論を述べる。

II. 論文審査結果の要旨

本論文は、「プロセス実行履歴」に基づく自動ドメイン定義と「拡張パラメータ」に基づくアクセス制御を用いて、ユーザが自分でポリシーの設定を行い、多様な環境下できめ細かなアクセス制御を実現し、さらにその成果を自らが開発する Linux OS に実装して実用に適したことが新規性と有用性の面で評価された。本研究は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が少なくない。

よって、本論文は、博士（情報学）の論文としては合格と認められる。

III. 審査経過

本審査委員会は、平成 23 年 2 月 3 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、博士論文として合格と判断した。その後、主査板倉征男の死亡にともない、主査を田中英彦に変更し副査に佐藤直を追加して、平成 24 年 3 月 12 日に最終試験を実施し、合格と判定した。