

論文内容の要旨

博士論文題目 動的保護が可能な動的構築機能を有するオペレーティングシステム・サーバに関する研究

氏 名 柏木 一彦

本論文は、計算機ハードウェア上に直に実装されたオペレーティングシステム（ベースOS）上で、ユーザにベースOSとは異なった仮想計算機環境を与える応用プログラム（OSサーバ）を対象として、これに動的保護が可能な動的構築機能を組み込む研究をまとめたものであり、具体的には以下の機能に関する内容を取り扱っている。

1)動的構築機能に関しては、OSサーバ実行中に新たな機能のOSサーバへの追加、追加した機能のOSサーバ内のカーネル空間への取り込み、カーネル空間へ取り込んだ機能のユーザ空間への追い出し、および追加した機能の新たな機能との置換を取り扱っている。取り込み機能により、OSサーバが行うシステムコールの処理を高速に実行できるとともに、上記の機能を組み合わせることにより、OSサーバを柔軟に構築でき、ユーザ環境に適した環境を提供できる。

2)動的保護に関しては、上記の取り込み、追い出しによるカーネル空間の動的な拡大、縮小に伴い、ユーザ空間からカーネル空間へアクセス不可とする機能を取り扱っている。本機能により、OSサーバプログラムをユーザプログラムから保護できる。

本論文は、序論・結論を含め10の章からなっている。

第1章では、本研究の背景、目的、およびその意義などを概説するとともに、本論文の構成を述べている。

第2章では、本研究の背景、目的、および意義を詳述している。具体的には、OSの構成法および実装レベルに関して、議論し、本研究で対象とするOSとして、マイクロカーネルアーキテクチャをとるOSサーバとすることを述べている。さらに、動的構築機能に関して、本研究で取り扱う機能を、システムサーバのカーネル空間への動的取り込みおよび追い出し、新たな機能の動的追加／取り込み／追い出し／置換、およびカーネルスケジューラの動的置換とすることを述べている。

第3章では、本研究で行う動的保護機能および動的構築機能について詳述している。

第4章では、本研究で行う動的構築機能を組み込む対象とするOSサーバモデルを述べている。具体的には、OSサーバの実行環境、OSサーバの内部アーキテクチャなどを述べている。

第5章では、上記OSサーバモデルに動的保護機能および動的構築機能を組み込むための検討課題を整理している。さらにこれらの課題を解決するための選択肢をいくつか提案するとともに考察を加え、本研究で採用する解決策を述べている。

第6章では、上記第5章で述べた解決策の具体的実現方法を述べている。

第7章では、第4章のOSサーバモデルとしてMINIX OSサーバをとりあげ、MINIX OSサーバへの実装方法を詳述し、実装している。

第8章では、実装したOSサーバについて、具体的に性能評価を行っている。その結果、システムサーバのカーネル空間への取り込みは効果があること、動的保護のオーバーヘッドはかなりあること、およびカーネルスケジューラの動的置換は効果があることを、定量的に実証している。

第9章では、関連研究について言及し、従来の研究と本研究との相違点を明確にしている。

第10章では、以上の研究成果についてまとめ、今後の課題を明らかにしている。

論文審査結果の要旨

本論文は、計算機ハードウェア上に直に実装されたオペレーティングシステム（ベースOS）上で、ユーザにベースOSとは異なった仮想計算機環境を与える応用プログラム（OSサーバ）を対象として、これに動的保護が可能な動的構築機能を組み込む方法を提案し、本機能の有効性を示したものである。具体的には、以下の機能を取り扱ったものである。

1. 動的構築機能： OSサーバ実行中に、i)新たな機能のOSサーバへの追加、ii)追加した機能のOSサーバ内のカーネル空間への取り込み、iii)カーネル空間へ取り込んだ機能のユーザ空間への追い出し、および、iv)追加した機能の新たな機能との置換。これらにより、OSサーバが行うシステムコールの処理を高速に実行できるとともに、OSサーバを柔軟に構築でき、ユーザ環境に適した環境を提供できる。
2. 動的保護： 上記の取り込み、追い出しによるカーネル空間の動的な拡大、縮小に伴い、ユーザ空間からカーネル空間へアクセス不可とする機能。本機能により、OSサーバプログラムをユーザプログラムから保護できる。

本論文の主な成果は以下に要約される。

1. 動的構築機能を組み込む対象とするOSアーキテクチャを分類し、それぞれの利点、欠点について考察を加えた。その結果、動的構築機能を組み込むOSアーキテクチャとしては、マイクロカーネルアーキテクチャをとるOSサーバモデルが適切であることを指摘した。

2. 動的構築機能を組み込む際の対象とするOSサーバモデルを仮定し、このモデルに動的構築機能を実現する際の検討課題を整理した。さらに、これらの検討課題に対する解決策としていくつかの選択肢を提案するとともに、考察を加え、本研究で採用する解決策を明らかにした。また、その実現に向けての具体的な方法を明らかにした。

3. 本研究で仮定したOSサーバモデルとなるMINIX OSサーバに、上記の実現方法を実装した。このとき、必要なデータ構造および処理など、具体的な実装方法を明らかにした。さらに、当該OSサーバの性能評価を行い、動的保護機能および動的構築機能の性能および有効性を明らかにした。具体的には、1)システムサーバのカーネル空間への取り込みにより、既存のシステムコールの実行時間が最大で約半分に減少されること、2)動的保護のオーバーヘッドは、動的保護のない場合に比べて約20倍とかなりのオーバーヘッドになること、3)カーネルスケジューラの動的置換の定量的効果、などを明らかにした。

以上のように、本論文は、ある環境下ではあるが、OSサーバに動的構築機能を組み込むことの有効性を定量的に示すとともに、動的保護機構の性能を定量的に示したもので、オペレーティングシステム分野において、学術上、実際上寄与するところが少なくない。よって、本論文は、博士（工学）の学位論文として価値あるものと認める。