論文審査の結果の要旨

氏名　品川 高廣

本論文は７つの章からなる．第１章は序論であり，本論文の研究の動機となった背景について論じている．近年，インターネットのような開放型分散環境では，匿名ユーザによる不正アクセスへの対処が重要な課題となっている．特に最近では，ウィルスやワームに代表されるように，不正なコードをネットワーク経由で送り込んでインターネット上の計算機に対して不正アクセスを行う攻撃が頻繁に行われており，このようなコードからローカルの計算機を保護する機構が不可欠になっている．しかし従来のオペレーティングシステムは主にLANのような閉じた環境を想定して設計されており，匿名ユーザからの攻撃を防ぐための強固な保護機構を実現することが難しくなっている．本論文では，オペレーティングシステムが提供する保護機構のモデルを再設計し，インターネットに接続された計算機上で安全に動作できるアプリケーションを作成するための基盤となる柔軟かつ効率の良い保護機構を提供することを目的としている．この主題の設定は，学位論文の主題として十分かつ妥当であると認められる．

本論文では，オペレーティングシステムの新しい抽象概念として，細粒度保護ドメインを提案している．細粒度保護ドメインとは，一つのプロセスの中に複数個持つことができる保護ドメインであり，プロセス内で動作するスレッドをアクセス権限が制限された環境で動作させることを可能にしている．細粒度保護ドメインを用いることによって，インターネットから送り込まれたコードに対してローカルの計算機資源に対するアクセスを制限し，不正アクセスによる被害を最小限に抑えることを可能にしている．また，保護ドメイン切り替えのコストを大幅に削減し，保護によるオーバーヘッドを低く抑えている．

第２章では，ソフトウェアによる保護機構に関する研究についてまとめている．従来の保護機構を，(1) オペレーティングシステムによるカーネルレベルのアプローチ，(2) 言語処理系などユーザレベルのソフトウェアによるアプローチの大きく２つに分けて，それぞれの方式における利害得失や本研究との位置づけについて述べている．

第３章では，本論文で提案する細粒度保護ドメインの概要およびその実現機構について述べている．従来の保護モデルではプロセスと一体になっていた保護ドメインの概念をプロセスから分離して，一つのプロセスに複数個の保護ドメインを持たせられるように拡張している．保護ドメインをプロセスから分離することによって，プロセスよりも細かい単位での柔軟な保護を可能にするとともに，スケジューリングなどを不要にして保護ドメイン切り替えのコストを大幅に削減している．また，細粒度保護ドメインをカーネルレベルで効率よく実現するために，(1) マルチプロテクションページテーブル，(2) システムコールフックの２つの技術から成る機構を提供している．マルチプロテクションページテーブルとは細粒度のメモリ保護を実現するためのカーネル内の抽象的な機構であり，システムコールフックはファイルなどのシステム資源に対する柔軟な保護を実現するための機構である．

第４章では，細粒度保護ドメインを既存のプロセッサ上で実装する技術について述べている．本論文では，主として最も普及しているプロセッサであるIA-32アーキテクチャ上での

実装について述べている．細粒度保護ドメインを効率よく実装するために，IA-32のセグメント機構を巧みに活用して，保護ドメイン切り替え時にTLBフラッシュ等のコストが発生しないように工夫している．また，セグメント機構の存在を意識せずに済むように，セグメントの配置を工夫してプログラマからは透過的に扱えるようにしている．さらに，IA-32のリング保護機構を活用することによって，頻繁使われる２つの保護ドメイン間の呼び出しを最適化する機構も実現している．

第５章では，細粒度保護ドメインの応用について述べている．細粒度保護ドメインを実際のアプリケーションに適用して，その汎用性・有用性を示している．応用例としては，(1) 実行可能コンテンツを安全に実行できるWebブラウザ，(2) インターネットアプリケーションのための軽量サンドボックス，(3) 特権コードを最小化したsetuidプログラムの３種類について，実際に設計および実装を行って実用性を示している．

第６章では，細粒度保護ドメインの性能を分析する実験の結果について述べている．細粒度保護ドメイン間の呼び出しにかかる時間を測定する実験を行い，103〜378プロセッササイクルという極めて高速な保護ドメイン間呼び出しが実現されていることを確認している．また，第５章で述べているアプリケーションを用いた実験を行って，保護によるオーバーヘッドがいずれも実用的なレベルに抑えられていることを示している．

第７章では，論文全体の内容をまとめ，今後の研究の方向性について述べている．

本学位論文は，開放型分散環境において安全なアプリケーションを構築するための基盤となるオペレーティングシステムの新しい保護モデルを提案し，その有効性について確認を行っている．細粒度保護ドメインという新しい抽象概念を提案し，その設計および実装を行うにとどまらず，複数の応用例を示して実際に細粒度保護ドメインを適用した実装を行い，その有用性について総合的に検証している点で，今後の関連分野の研究に寄与するところ大であると認められる．この点において，本論文は高く評価され，審査委員全員で，博士（理学）の学位を授与するにふさわしいと判断した．

なお本論文の一部は，共著論文として印刷公表済みであるが，論文提出者が主体となって研究および開発を行ったもので，論文提出者の寄与は十分である．