論文の内容の要旨

論文題目　A Kernel Support of Fine-grained Protection Domains
for Open Distributed Systems
(開放型分散システムのためのカーネルによる細粒度保護ドメイン)

氏　名　品川　高廣

インターネットのような開放型の分散環境では、セキュリティの確保が重要な課題である。従来のLAN等の閉じた環境とは異なり、開放型分散環境は匿名性が高いため，悪意を持ったユーザが存在する可能性がある．従って開放型分散システムでは、匿名ユーザによる不正アクセスからローカルのコンピュータ資源を保護するための機構が不可欠である。

インターネット接続環境の普及にともない、不正アクセスの手法も多様化している。従来はサーバマシンに侵入して不正アクセスを行なう手法が多かったが，近年ではクライアントマシンに対して任意のコードを送り込んで不正アクセスを行なう手法が増加している．コードを送り込む手段としては，Javaアプレットや ActiveX などの実行可能コンテンツとして送り込む方法の他に，PDFや Postscript 等のように一見静的なコンテンツの中にコードを埋め込んで送り込む手法も存在する．この手法では、バッファ溢れ攻撃などを用いることで，埋め込んだコードを閲覧プログラムの権限で実行させることができる。このような不

正アクセスの手法の多様化に対応するためには，様々なプログラムに対して保護機構を組み込む必要がある．

しかし従来のオペレーティングシステムは、このような不正アクセスに対して十分な保護機構を提供していない。これは，従来のプロセスによる保護モデルが基本的にLAN等の閉じた環境を想定して設計されており、開放型分散環境のように匿名ユーザが作成したコードを実行するような状況は想定していないためである．例えば、プロセスによる保護では，ActiveXなどの実行可能コンテンツに対して，通常よりもアクセス権を制限して実行するといったことは難しい．また、プロセスによる保護はプロセス間通信のコストが大きいため，保護のオーバーヘッドが非常に大きくなってしまう。本研究の実験では、実行可能コンテンツの保護にプロセスを用いると，約102%ものオーバーヘッドが生じるという結果が出ている。従って、開放型分散システムのための保護機構では、アクセス権限を細かく設定できる柔軟性と、保護ドメイン間の通信を効率よく行える高い性能を合わせ持った保護機構が必要ある。

従来の研究でも、オペレーティングシステムのカーネルを拡張して保護機構を強化する試みが行われている．しかしこれらの研究では、保護機構が特定の目的に特化されたものが多い。カーネルによる保護機構は，様々なプログラムで用いられるものであるので、特定の目的に特化したものではなく汎用的な機構であることが望ましい。また，言語処理系の機能によりユーザレベルで保護機構を実現する研究も数多く行なわれているが，既存のバイナリに対して十分な保護を行なうことは難しい．

本論文では、オペレーティングシステムの保護モデルにおける新しい概念である**細粒度保護ドメイン**を提案する。細粒度保護ドメインとは、従来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の保護ドメインを持てるようにしたものである。細粒度保護ドメインを用いると、一つのプロセス内のコードを異なるアクセス権限で実行させることができる。例えばプロセス内でメモリ保護を行うために、細粒度保護ドメインごとにページ単位で異なるメモリ保護モードを設定することができる。また、ファイルやネットワークに対して，より制限されたアクセス権限を設定することができる。

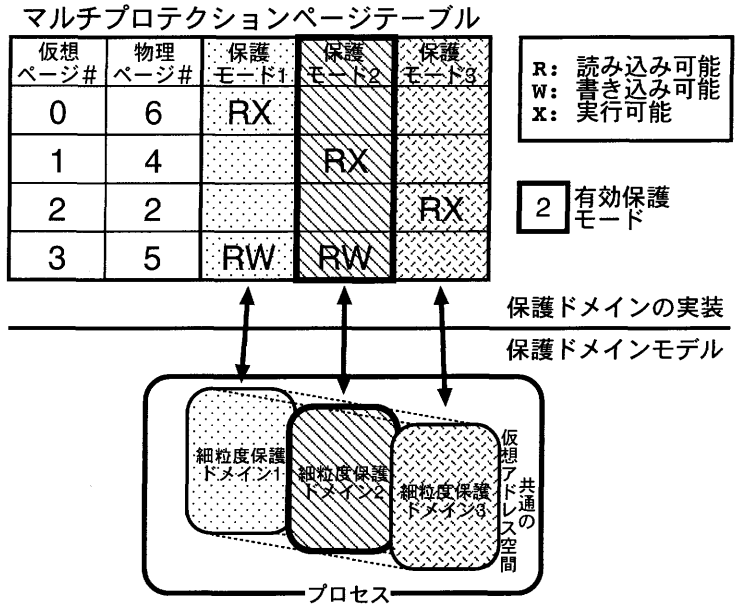

図 1: 細粒度保護ドメインとマルチプロテクションページテーブル

これによって、悪意を持ったユーザによって送り込まれた可能性のあるコードに対するアクセス権限を制限して，不正アクセスを未然に防止することができる．

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，本論文では**マルチプロテクションページテーブル**と呼ばれる仮想的な機構を導入する（図 1 参照)。マルチプロテクションページテーブルとは、従来のページテーブルを拡張して、一つのページエントリに対して複数個の保護モードを設定できるようにしたものである。ある時点では複数個の保護モードのうちの一つだけが有効であり、保護ドメインの切り替えと連動して有効な保護モードが切り替わる。マルチプロテクションページテーブルを利用すると，同じ仮想アドレス空間を共有しながらも細粒度保護ドメインごとに異なるページ保護モードを持たせることが可能になる．また保護ドメインの切り替え時にページテーブルを切り替える必要が無いため，TLB フラッシュなどを避けて軽量な保護ドメイン切り替えを提供できる．また，軽量な保護ドメイン切り替えをベースにシステムコール横取り機構を実現することで、ファイルなどの資源に対してユーザーレベルで柔軟かつ効率の

良いアクセス制御が可能になる.

マルチプロテクションページテーブルを既存のプロセッサ上で実装するためには，プロセッサごとに異なる手法を用いる．本論文では、特にインテルのIA-32アーキテクチャ上での実装について詳しく説明する．IA-32は世界中で最も多く使われているプロセッサのアーキテクチャであり、その上での実装を示すことは細粒度保護ドメインの実用性を示す意味で重要である。本論文で述べる実装では、IA-32アーキテクチャのセグメント機構とリングプロテクション機構を活用することにより、マルチプロテクションページテーブルの効率の良い実装を実現している.

細粒度保護ドメインの有用性を実証するために、本論文では三種類のアプリケーションに対して細粒度保護ドメインを適用した例を示す。一つ目は、実行可能コンテンツをWebブラウザ内で安全に実行する環境である。実行可能コンテンツに対して細粒度保護ドメインを割り当てることで、実行可能コンテンツによる不正アクセスを防止する。二つ目は、柔軟でかつ効率の良い汎用サンドボックス機構である。細粒度保護ドメインを用いることで，サンドボックスのリファレンスモニタをユーザレベルで実装しつつも，保護のオーバーヘッドを低く抑えることができる．三つ目は、特権コードを最小化したsetuidプログラムである。細粒度保護ドメインを活用してsetuidプログラム中の本当に必要なコードにのみroot権限を与えることで、setuidを乗っ取ることによるroot権限の不正取得が行われる可能性を減らす。これらのアプリケーション例を通じて、細粒度保護ドメイン機構の有効性を検証する.

また，細粒度保護ドメインの性能を検証するために、IA-32アーキテクチャ上での実装を用いた性能実験の結果を示す。細粒度保護ドメイン間呼び出しにかかる時間の測定結果はPentiumプロセッサ上で103サイクルであり，極めて高速な保護ドメイン間呼び出しが実現できることを確認した．また、実際のアプリケーションを用いてオーバーヘッドを測定した結果、マンデルブロ集合を描く実行可能コンテンツでは平均22.6%、サンドボックスしたAcrobat Readerでは約1.5%、特権コードを最小化したpasswdコマンドでは3.8%程度であることがわかった。