5Z−2

オブジェクト/スレッドモデルオペレーティングシステムにおける柔軟できめの細かい保護機構の設計

繁田 聡一 † 芦原 評 ‡ 岡本 秀輔 † 清水 謙多郎 § 曽和 将容 †

† 電気通信大学 情報システム学研究科, ‡ 電気通信大学 情報工学科, § 東京大学 農学生命科学研究科

1. はじめに

互いに協調する細粒度オブジェクトによって構成されるオブジェクト/スレッドモデルのオペレーティングシステム [2] において、オブジェクトの柔軟な保護を実現する機構を提案する。オブジェクトとはデータとメソッドをカプセル化したものであり、スレッドとはプログラムコードの実行主体である。複数のオブジェクトが同一のアドレス空間上にマッピングされ、それらのオブジェクトが提供するメソッドを複数のスレッドが利用する。そのため、一様な手続き呼び出しの手順でオブジェクトを呼び出すことができるが、オブジェクトは同一のアドレス空間上で不当なアクセスから互いに保護されなければならない [1]。したがって、アクセス権を規定しオブジェクト呼び出しを制御する機構と、実行時の不正なメモリ参照を防止する機構とが必要である。本稿では、前者について、キー/ロック方式 [3] に基づいた方式を提案する。

2. 提案方式

2.1 特 徴

提案方式は、アクセス制御リスト方式とケイパビリティー方式の両者の特徴を合わせ持つキー/ロック方式に基づいている。従来のキー/ロック方式の持つ長所を活かし、短所を改善することによって柔軟な保護の実現を目指している。

改善された点

- スレッドはオブジェクト呼び出しの際に複数のキーを利用できる。また、オブジェクトの Lock List には複数のキーの組み合わせを指定することができ、それらを全て提示できるスレッドにのみアクセスを許すことができる。すなわち、アクセスを許す条件をキーの組合せによって柔軟に指定できる。
  - 従来の方式では、複数のキーを用いたアクセス条件の指定ができない。
- スレッドが呼び出し可能なオブジェクトとメソッドを明示的に限定する SCL 機構を導入し、挙動が不審な信頼できないプログラムをユーザが安全にテストできるようにしている。
  - 従来の方式では、サブジェクトが、どのオブジェクトへのどのような操作が許されているのかを把握することは困難である。

従来の方式からの長所

- オブジェクトがアクセス権を管理するため、アクセス権の取消しや変更が容易である。
- キーの貸与や譲渡により、アクセス権の貸与や譲渡が可能である。

従来の方式からの (改善されていない) 短所

- キーの偽造を防止しなければならない。
- アクセスのたびにロックリストを検索するコストがかかる。

2.2 キー

提案方式では、3種類のキーを用意する。スレッドが誰の権限で実行されているのかという基本的な権限を表すためにユーザキーを用意する。また、スレッドがどのオブジェクトを呼び出しているのかによってスレッドの状態を表すことにし、その実現のために個々のオブジェクトに与えるオブジェクトキーを用意する。また、ユーザが必要に応じて利用できるキーとして、ユーザデファインドキーを用意する。

- ユーザキー：ユーザの識別子であり、ユーザを単位としたアクセス条件を設定するために用いる。また、スレッドやオブジェクトのオーナーを表すためにも用いる。

"A Flexible and Fine-grained Protection Mechanism in Object/Thread Model Operating Systems"

Soichi Shigeta†, Hyo Ashihara‡, Shusuke Okamoto†, Kentaro Shimizu§, and Masahiro Sowa†

†The Graduate School of Information Systems, The University of Electro-Communications
1-5-1, Chofugaoka, Chofu-shi, Tokyo 182, Japan.

‡Department of Computer Science, The University of Electro-Communications

§The Graduate School of Agricultural and Life Sciences, University of Tokyo
1-1-1, Yayoi, Bunkyo-ku, Tokyo 113, Japan.

- オブジェクトキー：個々のオブジェクトに与えられる。クラスの持つオブジェクトキーは、インスタンスに継承される。クラスに与えられたオブジェクトキーを用いてクラスを単位としたアクセス条件の設定を、インスタンスに与えられたオブジェクトキーを用いてインスタンスを単位としたアクセス条件の設定を行なう。
- ユーザデファインドキー：ユーザが任意のオブジェクトのグループに同じアクセス権を設定したい場合に、明示的に生成して用いる。

2.3 ロック

各オブジェクトは、どのスレッドにどのメソッド呼び出しを許すかを規定する Lock List を持つ。Lock List の設定を変更できるのはオブジェクトのオーナーだけである。Lock List の各エントリは、<キーの論理式, メソッドの集合, メソッドの実行に関する指定 (許可, 禁止)> で構成される。Lock List の設定に際し、複数のキー間に AND を指定することでキーを割符として用いることができる点が提案方式の重要な特徴である。

2.4 アクセス権の判定

スレッドは、スレッドキーリストにキーを保持する。また、オブジェクトは、そのオブジェクトを実行しているスレッドが別のオブジェクトを呼び出す際に使用することを許すキーをオブジェクトキーリストに保持する。オブジェクトの生成時には、システムによって与えられたオブジェクトキーだけがオブジェクトキーリストに設定されている。オブジェクトのオーナーは、ユーザデファインドキーを追加することができる。

スレッドがオブジェクトを呼び出すとき、システムはオブジェクトの Lock List を参照してスレッドがキーリストに保持しているキーとマッチするエントリを探索し、そのエントリに実行しようとするメソッドが記載されていればメソッドの呼び出しを許す。

提案方式でキーを割符として用いる例を図１に示す。Database file の write メソッドの呼び出しは、K_{foo} と K_{DM} の２つのキーを併せて提示できるスレッドにだけ許されるように Lock List が設定されている。したがって、ユーザ *foo* の権限で実行されているスレッド (K_{foo} を持っている) が Database manager を呼び出し、Database manager のスレッドキーリストに設定されているオブジェクトキー K_{DM} と併せて提示できる場合に限り Database file の write メソッドの呼び出しが許可される。例えば、thread1 はユーザ *foo* の権限で実行されているが K_{DM} を提示できず、Database file のメソッド呼び出しは許されない。また、thread3 は K_{DM} を利用することはできるが、ユーザ *bar* の権限で実行されているため K_{foo} を提示できず、Database file の write メソッドの呼び出しは許されない。

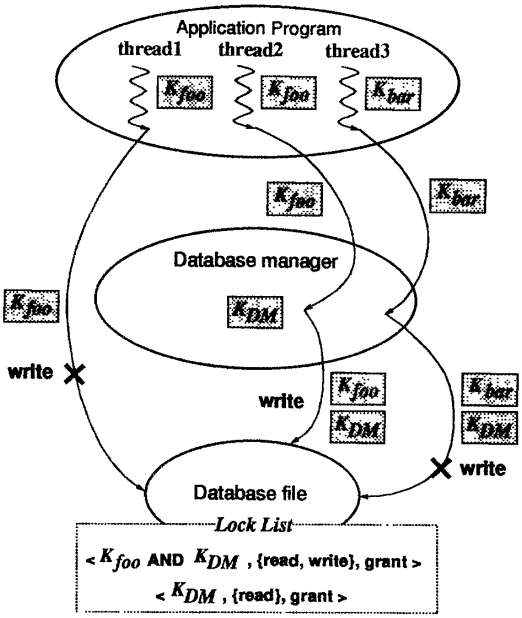

図 1: 割符としての使用例

2.5 Subject Control List (SCL)

挙動の不明な信頼できないコードをユーザが安全にテストするための機構である。ユーザは、オブジェクトに SCL を設定して、そのオブジェクトを実行するスレッドが呼び出し可能なオブジェクトとメソッドを予め明示的に限定することができる。SCL の各エントリは、<オブジェクト名, メソッドの集合>で構成される。SCL は Lock List に先立ってチェックされる。

3. まとめ

キー/ロック方式に基づいた柔軟なオブジェクトの保護機構を提案した。提案方式の有用性の検証と効率的な実現が今後の課題である。

参考文献

[1] J. S. Chase, H. M. Levy, M. J. Feeley, and E. D. Lazowska, "Sharing and Protection in a Single Address Space Operating System", *ACM Transactions on Computer Systems*, **12**, 4, pp.271-307 (1994).

[2] G. Hamilton and P. Kougiouris, "The Spring Nucleus: A mikrokernel for objects", *Proceedings of Summer USENIX Technical Conference*, pp.147-159 (1993).

[3] 前川 守, 所 真理雄, 清水 謙多郎, 分散オペレーティングシステム, 共立出版 (1991).