スレッド別ページ保護機能の検討

山崎智広† 池田貴広†
千葉雄司†† 土居範久†

1. はじめに

近年，情報システムは社会の重要なインフラとなっており，情報システムの障害は，社会に大きな悪影響を与える．このため，特に銀行業務などのミッションクリティカル分野では迅速な障害対応が重要になるが，複雑化した情報システムにおける障害原因の究明は容易でなく，原因究明を支援する技術が求められている．

本論文では，原因の究明に長い時間がかかりやすい障害の 1 つであるメモリ破壊を対象として，原因究明を支援する技術を検討する．メモリ破壊の原因究明に長い時間がかかりやすい理由は，次の 2 つである．

(1) メモリ破壊の発生直後にシステムダウンなどの障害が発生するとは限らないため．メモリ破壊の発生直後にシステムがダウンした場合には，ダウン時のプログラムカウンタの値から破壊の原因を容易に推定できるが，発生から長期間が経過すると，プログラムカウンタの値を推定の手掛りにできなくなる．

(2) 破壊されたメモリ領域を管理するソフトウェア製品と，破壊の原因となったソフトウェア製品が必ずしも一致しないため．複数のソフトウェア製品からなるプログラムにおける障害の原因調査を効率的におこなうには，障害の原因となったソフトウェア製品を正しく推定し，推定したソフトウェア製品の開発部隊に調査を依頼する必要があるが，メモリ破壊ではこの推定が容易でない．往々にして破壊されたメモリ領域を管理するソフトウェア製品の開発部隊に調査依頼が出されるが，破壊の原因が別のソフトウェア製品にある場合も多く，このとき開発部隊間の組織的な壁もあって原因調査が長期化しやすい．

† 中央大学理工学部情報工学科
Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University
†† 中央大学研究開発機構
Research and Development Initiative, Chuo University

2. スレッド別メモリ保護機能

（2）の問題を防ぐ手段として，ページ保護の機能を用い，個々のソフトウェア製品が提供する機械コードの実行時に，他のソフトウェア製品の管理下にあるメモリ領域を参照不能にする方法が考えられる．この方法によれば，あるソフトウェア製品中のバグが，他のソフトウェア製品の管理下にあるメモリ領域を破壊しようとすると，即刻ページトラップが発生するので，バグの所在を簡単に把握可能になる．ソフトウェアの実行に際して参照できるメモリ領域を最低限に絞ることには，セキュリティを向上する効果も期待できる．しかしながら，この方法の実用化を阻む問題が，現行の OS が提供するスレッドの実装にある．その問題とは，１つのプロセスに属する全スレッドが，ページの読書権限を共有していることである．スレッドがページの読書権限を共有している状況下では，あるスレッドがソフトウェア製品の提供する機械コードの実行にあたって，別のソフトウェア製品の管理下にあるメモリ領域を参照不能にすると，その影響が別のソフトウェア製品の提供する機械コードを実行中のスレッドにまで及んでしまう．この問題の解決を目的として，本研究では，ページ保護の機能をスレッドごとに提供する技法を Linux および T-Kernel 向けに実現し，評価を試みる．

3. 結　　論

スレッド別ページ保護機能の実現を試みている．スレッドごとに異なるメモリ参照権限を与えるという思想は新しくないが[1]，実際的な評価によって，スレッド別ページ保護機能の実用性を検討する予定である．

参考文献

1) Chase, J. S., et. al.: Sharing and Protection in a Single-Address-Space Operating System, *ACM Transactions on Computer System*, Vol. 12, No. 4, pp. 271–307 (1994).