論文審査の結果の要旨

氏名　光來健一

近年のソフトウェアの複雑化・肥大化に伴い、ソフトウェアはインターネットからの攻撃や不安定なソフトウェアの存在などの安全面における問題を抱えている。これらの問題の主な原因はソフトウェアの不具合であるが、現状ではソフトウェアから全ての不具合を除去するのは難しい。そのため、万一不具合のせいでソフトウェアが異常な動作をした場合でも被害をできるだけ抑えることができるセーフティネットが利用されてきている。セーフティネットとはソフトウェアの異常な動作を検出するための防衛ラインである。不具合の被害を常に最小に抑えるには、サーバを利用するクライアントやオペレーティングシステム (OS) モジュールの安定度に応じて、セーフティネットの適用範囲が変更可能であるのが望ましい。しかし、セーフティネットの適用範囲を動的に変更するには、安全性や性能の点で問題があった。本研究では、OSのサポートにより安全に、かつ、性能をできるだけ犠牲にせずに、セーフティネットの適用範囲を変更できるシステムを設計し実装することを目標としている。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。

本論文は6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について論じている。

第2章は動的なセーフティネットを実現するための問題について、従来の研究をサーベイするとともに、詳しい分析を行っている。本研究では、クライアントに応じてサーバのセーフティネットを変更する場合と、OSモジュールの安定度に応じてセーフティネットを変更する場合を対象としている。クライアントに応じたセーフティネットの変更は、万一攻撃された場合でも常に被害を最小に抑えるのに役立つ。しかし、乗っ取られたサーバにセーフティネットの変更を許してしまうと危険である。一方、OSモジュールの安定度に応じたセーフティネットの変更は、安全性と性能のトレードオフを取ることを可能にする。しかし、この変更をユーザに透過にし、かつ、性能を犠牲にしないようにするのは容易ではない。それぞれの動的なセーフティネットの実現方法について以下の3章と4章で説明している。

第3章ではサーバプロセスに対して動的なセーフティネットを実現するためのアクセス制御機構について述べている。サーバプロセスにアクセス制限の変更を許すために、サーバプロセスから攻撃の影響を除去するプロセスクリーニングという手法を提案している。この手法を用いることにより、セーフティネットの範

囲を動的に変更する場合の安全性を確保している。また、クライアントを正しく判定し、サーバに適切なアクセス制限をかけられるようにするために、クライアントの行動の追跡や、ネットワークレベルでのユーザ認証を行っている。

第4章ではOSモジュールに対して動的なセーフティネットを実現するための保護機構について述べている。OSモジュールの安定度に応じた保護レベルの変更を許すために、マルチレベル・プロテクションという機構を提案している。この機構はOSモジュールに変更を加えることなく保護レベルを変更することを可能にしている。さらに、保護レベルを最小にした時に余分なオーバヘッドがかからないように注意深くシステムを設計することにより、性能が犠牲にならないようにしている。

第5章では3章と4章で述べたシステムの性能を測定し、実験結果についての考察を行っている。まず、安全にサーバのアクセス制限の変更を行うために使われるプロセスクリーニングのオーバヘッドを、ウェブサーバを対象にして測定している。その結果、従来の手法を用いるより高速化できていることが示されている。次に、作成したOSモジュールについてマルチレベル・プロテクションを用いることにより、安全性と性能のトレードオフが取れていることを示している。

第6章は論文全体の内容をまとめ、今後の研究課題について論じている。本論文の成果は、性能について十分考慮した上で動的なセーフティネットを実現した点にあることが述べられている。さらに、より粒度の細かい処理が要求されるミドルウェアへのプロセスクリーニングの適用、およびマルチレベル・プロテクションにおける保護レベルの変更の指針について議論されている。

本学位論文は、ソフトウェアの安全面での問題を緩和するために、動的なセーフティネットの設計と実装方法について提案したものであり、安全性と性能の点からその有用性を検証している。性能をできるだけ低下させずに、状況に応じて適切なセーフティネットを構築することを可能にした点で、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。

なお、本論文の内容の一部は、千葉 滋・益田 隆司との共同研究であるが、論文提出者が主体となって研究および開発を行なったもので、論文提出者の寄与が十分であると判断する。

したがって、博士（理学）の学位を授与できると認める。