

氏名(本籍)	あ べ ひろ たけ 阿 部 洋 文 (新潟県)
学位の種類	博 士 (工 学)
学位記番号	博 甲 第 3421 号
学位授与年月日	平成 16 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
審査研究科	工学研究科
学位論文題目	プログラム実行および WWW 利用の安全性に関する研究

主 査	筑波大学教授	理学博士	板 野 肯 三
副 査	筑波大学教授	工学博士	岡 本 栄 司
副 査	筑波大学教授	理学博士	佐 藤 三 久
副 査	筑波大学教授	Ph. D.	田 中 二 郎
副 査	筑波大学助教授	博士(理学)	加 藤 和 彦

## 論 文 の 内 容 の 要 旨

本研究の目的は、既存のソフトウェアを用いる場合に生じる安全性上の問題点を解消することである。本研究の成果は、次の三点である。

第一に、プログラムの実行が外部の攻撃者によって万が一乗っ取られてしまった場合の被害を防ぐためのシステムを設計し、実現を行った。本方式は、プログラム中の関数呼び出しに着目し、特定の関数呼び出しが実行された時点で、プログラムに与えられるアクセス権限を動的に切り替える。それにより、万が一プログラムの実行が乗っ取られたとしても、プログラムの持つすべての権限が奪われることを防ぐことが可能になる。本システムは、プログラムの実行を監視するリファレンスモニタ部と、動的に切り替わるポリシーの記述の作成を支援する GUI ツールで構成される。本研究では、本提案方式を用いてプログラムを実行した場合の実行時オーバーヘッドについて計測を行った。

第二に、精度が高くオーバーヘッドがより少ない侵入検知システムの実現を行った。本研究では、既存の侵入検知手法の中で、精度が高いがオーバーヘッドが非常に大きかった手法を取り上げ、その手法を高速化することで精度が高くオーバーヘッドがより少ないシステムの実現を行った。本研究における高速化は、主に、監視対象のプログラムの実行時スタックを異常検知に利用することと、実行可能パスの探索結果を蓄積して再利用することによって達成された。本研究では、提案する手法を用いて異常検知システムを実現し、実際のプログラムを用いた実験を通して、高速化手法の効果が十分に得られていることを示した。

第三に、WWW 利用時のプライバシーを実現するための匿名プロキシに着目し、集中型のサーバを必要としない匿名分散プロキシを設計し、実現を行った。本方式では、匿名プロキシ間の通信に Peer-to-Peer 型の分散システム用に開発された通信プロトコルを利用した。それにより、集中型サーバが存在しなくても互いに通信を行うことが可能となった。また、その Peer-to-Peer 用通信プロトコルを利用する場合に生じる匿名性上の問題について考察し、それを解決する手法を提案した。本研究では、提案手法を用いた場合の通信遅延について、ネットワークシミュレータを用いて考察を行った。

## 審査の結果の要旨

本論文は、セキュリティ上の脆弱性がアプリケーションプログラムにある場合にでも被害を最小化するシステム、精度高く実用的なオーバーヘッドで実行可能な侵入検知システム、完全分散型アルゴリズムによる匿名性提供プロキシ、という三つの新方式を報告したものである。現在、社会的な問題となっているセキュリティおよびプライバシー問題に対して正面から取り組み、新方式の提案、実装、評価を行っている点は高く評価できる。匿名性を提供する技術の取り扱いについては注意も必要であるが、未開拓の分野の問題に果敢に取り組んでいる研究姿勢は大いに評価できる。

よって、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。