実施企業名：株式会社　三菱総合研究所
研究課題名：静的解析によるＣ／Ｃ＋＋プログラムのバッファオーバーフロー検出技術

1. 研究の概要

情報セキュリティ上の脆弱性原因の中で、C/C++プログラムに潜在するバッファオーバーフロー脆弱性原因は最も重大な脆弱性原因である。この脆弱性原因は、プロセス乗っ取りを攻撃者に許す等、もたらす被害は極めて深刻であり、脆弱性報告サイトでも報告数は突出して多い。この脆弱性原因の検出に関する既存の手法・ツールはいずれも根本的な欠点を持ち、決定的な解決手段とはなっていない。

採択企業はこれまでに、既存の手法・ツールの欠点を全てクリアする新しい検出用静的解析手法のスキームを研究開発し、その有効性をＣプログラムにおいて確認した。今回、これを改良し、また、C++プログラムも対象とするものに拡張する研究開発を行い、さらにそれを実装する研究開発を行って、静的解析による C/C++バッファオーバーフロー検出ツールを開発する。

2. 研究目標の達成状況と実用化への展望

当初の研究目標に対し一定の成果が得られ、実用化の可能性も期待できる。

□　研究目標の達成状況

研究目標	達成状況
静的解析による C/C++バッファオーバーフロー検出ツールを開発する。また、プロジェクトを通して得た知見をまとめ、セキュアプログラミングガイドラインを作成する。	左記に掲げた目標を達成し、ソースコード静的解析によるバッファオーバーフロー検出ツールを開発した。また、本研究開発で得られた知見をガイドラインにまとめた。

□　採択企業における実用化への展望

今後は、本ツールの実装を洗練させ、採択企業グループが展開していく総合的な情報セキュリティサービスの一環としてツールキット化し、言語処理系への組込みや単体としての売り出しやコンサルティングといった有償実用化への展望を図るとしている。また、特に教育関連を中心に無償版を提供することも、普及活動の一つとして考えているとのことである。

3. 総合所見

《総合》

当初の研究目標に対し一定の成果が得られ、実用化の可能性も期待できる。

本研究では、ネットワーク等から進入する不正なアクセスの高度化に対処すべく、プログラミングの開発段階で C/C++プログラムに潜むセキュリティ問題を検証する「静的解析によるバッファオーバーフロー検出ツール」の開発、当該ツールの普及に向けての「セキュアプログラミングガイドライン」の作成などが行われた。その結果、試用に供しうるツールができて、その効果実証の段階に入っていると認められることから、初期の開発意図は達成されたと評価する。しかしながら、本検出ツールに対するユーザ評価が不十分なため、実用性や他のツールに対する優位性を評価するには至っていない。

今後、ユーザ評価を積極的に行い、ユーザ側からのフィードバックを通して問題点や残された課題について整理し、本ツールの実用性の評価を確実に行うと共に、展開していく総合的な情報セキュリティサービスの中で、本ツールが十分に活用されることを期待する。また、情報セキュリティ向上という社会性の高いテーマを扱っていることから、ソフトウェア技術者の教育などにも展開し、実社会で広く活用されることを大いに期待する。

《詳細》

ネットワークから進入する不正なアクセスは、高度化してきており、この危険をプログラミングの開発段階で検証することを目指す本研究の意義は大きい。研究の成果についても初期の開発意図は達成されたと評価する。具体的には、バッファオーバーフローの発生要因を体系的網羅的に解析し、その要因事項を満たすソースコードの静的解析による検出技術を開発し、検出ツールに実装したことで、試用に供しうるツール作成が完了した。現在は実用化に向けた実証フェーズに位置しているといえる。今後は、検証テストを積み重ね、ユーザからのフィードバックをもとに本ツールを評価し、実用化に向けた検出精度の検証や操作性の向上などに努めてほしい。

知的財産に関しては、本研究開始前に関連する特許を出願済みではあるが、本研究成果としての特許出願は行われていない。本技術の優位性を確保するためにも、早期に周辺技術に関しても特許出願されることを期待する。

事業化に関しては、本研究成果のツールとしての技術的な実用性と IT セキュリティ分野のニーズから事業化が可能と思われる。ただし、事業化を進めていく上で、本ツールの精度検証や操作性など技術的な課題の洗い出しとその克服とともに、実際の市場規模を調査し、本ツールを活用した明確な事業モデルの設定が必要である。これらの点を考慮して、会社として早急に事業化に踏み切ることを期待する。

C/C++プログラミング言語は、組み込みソフトウェアなどに現在及び将来的にも利用されると予測でき、そのセキュリティ対策として本技術の利用価値はソフトウェアの信頼性を高めるために有用であり、本ツールは IT セキュリティに係る新たなサービス事業の可能性を秘めている。また、ソフトウェア技術者の教育などにも活用できるため、IT 教育機関等への無償提供を含め、本研究成果が実社会で広く活用されることを大いに期待する。