博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　セキュア・アプリケーション開発のためのアスペクト指向フレームワーク
申請者　　：　大久保隆夫
審査委員会　：　主査　教授　田中英彦
副査　教授　小柳和子
副査　教授　松尾和人
副査　准教授　辻　秀典
副査　助教　金　美羅

Ⅰ．論文内容の要旨

本論文は、「セキュア・アプリケーション開発のためのアスペクト指向フレームワーク」と題し、10 章と付録からなる。情報システムは情報社会の重要な基盤であるが、最近は、情報システムやそれが提供するサービスへの様々な攻撃の脅威が高まっている。このような攻撃によって被害を受ける原因の多くは、システムのアプリケーションにその対策が十分施されていないことである。従って、情報システムを構成するアプリケーションをセキュアに開発する手法が重要であるが、従来その方法には確立されたものが無かった。本論文は、このようなセキュアなソフトウエア開発を確実に、且つ効率的におこなう手法について論じたものである。

第 2 章は「セキュアなアプリケーション開発の問題点と従来技術」で、セキュアなアプリケーション開発の問題点は、開発に携わる関係者のセキュリティ知識が不足していることと、既存のソフトウエア開発手法は、想定されない利用や振る舞いへの観点が欠落しているため、セキュアなソフトウエア開発に必ずしも適合しないこと、更に、既存技術は開発各工程に閉じており、工程間の連携が不足していることであると述べている。

第 3 章は「アスペクト指向フレームワーク“Security Injector”の提案」で、2 章で述べた問題点を解決する手法として、セキュリティ関心事およびその実現を一般の開発者から分離して開発を行うアスペクト指向のプロセスと、そのプロセスを効率的に実現するために、要求分析、設計、実装、テストの各工程毎に導入した開発支援手法からなる開発のフレームワークを提案している。

第 4 章は「Security Injector: 要求分析の要素技術」で、まず、セキュリティ関心事と非セキュリティ関心事とを分離するプロセスとして、アスペクト指向セキュリティ要求策定プロセス AOSRE を導入し、通常の開発者とセキュリティ有識者との間で仕事を分離し、各者が独立して行う作業と、協力して行う作業とに分けて開発を進める手法を与えている。次に、開発各工程の最初である要求分析を支援するために、セキュリティ有識者が担当する作業である脅威分析と対策抽出における作業を容易化する手法として、資産ベースのミスユースケース手法 AsseMis を提案している。これは、従来のミスユースケースに、保護資産の表記、ミスユースケースと資産の対応付け、アーキテクチャ情報追加、ミスアクタの拡張などを施し、脅威分析を容易化するとともに、対策案を漏れなく抽出することを可能ならしめる手法である。

第 5 章は「Security Injector: 設計の要素技術」で、要求分析工程で分離された作業に従って、一般開発者とセキュリティ有識者とが各自の仕事に専念して開発が出来ることを保証するために、セキュリティを必要な箇所に適切に挿入する仕組みとして、依存性注入（Dependency Injection）に基づく関心事横断点の設計と制約の導入手法を与えている。更に、セキュリティ関心事の設計を効率化するために、セキュリティ設計のパターン化による再利用を図ってお

り、ロールベースアクセス制御、状態遷移に基づくアクセス制御、などのパターンを提案している。

第 6 章は「Security Injector: 実装・テストの要素技術」で、設計工程で定めた関心事の横断点に正しくセキュリティが挿入されるとともに、実装時に脆弱性が混入されないことを保証する手法を与えている。すなわち、関心事の横断点となるメソッド呼び出しのメソッド名に特徴的な命名規則を設け、その命名規則に従った形でソースコードを自動生成するとともに、自動生成された非セキュリティ関心事側の特徴点を変更できないようにするための制約を導入している。また、セキュリティ関心事をライブラリ化して開発効率を上げるとともに、実装時の脆弱性の混入を防いでいる。更に、テスト段階のセキュリティの確認を容易化するために、制約に基づくテスト手法を導入している。

第 7 章は「ケーススタディ」で、Web アプリケーションを例にケーススタディを行った結果を示している。対象のアプリケーションは Web のブックストアで、本の検索、注文、管理が可能なものであり、この開発に Security Injector を利用した場合、狙い通りに非セキュリティ関心事とセキュリティ関心事とが分離され、且つセキュリティが要求定義通りに実現されることを確認している。

第 8 章は「評価」で、開発手法として様々な観点から本方式を評価したものである。まず、実装工程における脆弱性の排除を狙ったインジェクション防止ライブラリを評価し、それが他の手法と比較して、攻撃の検出や防止の点でより優れていることを示している。仕事の分離に関しては、それによってセキュリティ作業量が従来手法に比して数分の一程度に減少すること、また、パターンを用いることで作業量が著しく減少することなどを実際に 11 個のアプリケーション開発を元に示し、本手法が優れていることを示している。更に、従来技術が工程毎に独立していたのに対し、本手法では、前工程の結果を後工程で利用することが可能で、作業効率が上がることを分析している。

第 9 章は「議論と検討」で、本研究で達成したことをまとめるとともに、未解決の問題や今後の課題について述べている。

第 10 章は「結論」である。

Ⅱ. 論文審査結果の要旨

これを要するに本論文は、情報社会を支える様々な情報システムを構成する上で重要な、セキュアなソフトウエア開発を効率よく、また、確実におこなうための開発フレームワークを与え、その効果を具体的に評価したもので、情報学に貢献するところ少なくない。

よって、本論文は、博士（情報学）の学位請求論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、2009 年 2 月 2 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。