研究成果展開事業　研究成果最適展開支援プログラム
FS ステージ　シーズ顕在化タイプ　事後評価報告書

研究開発課題名	：	動的情報追跡による注入攻撃の普遍的な検出方式の実用化
プロジェクトリーダー 所　属　機　関	：	（株）情報技研
研　究　責　任　者	：	五島正裕（国立情報学研究所）

1. 研究開発の目的

情報システムは非常に重要な社会基盤であり、そのセキュリティ確保は必要不可欠である。情報システムを支えるサーバに対する攻撃のうち、今なお実に半数以上が Web アプリケーションに対する注入攻撃（インジェクション・アタック）である。これだけ大きな問題である注入攻撃にもかかわらず、現在の脆弱性対策は対処療法的で根本的な対策がなされていない。

本研究開発では、注入攻撃の本質に注目し、シーズ候補である SWIFT を用いて、普遍的な検出方式が実用的に応用可能であることを検証することを目的としている。重視する点は、SWIFT という普遍的な検出方式が、実際に世の中で使われている一般アプリケーションに適用したときに有効であることを示し、一般に応用可能であることを検証することにある。

2. 研究開発の概要

①成果

SWIFT が組み込まれた言語処理系において、実際にサーバサイド・アプリケーションを実行し、スクリプト・インジェクション・アタックが実用環境で検出・防御ことを確認することである。

そのためには、SWIFT で伝播される汚染情報を元に、外部へ引き渡される文字列のチェックする機構が必要となる。そこで、外部に引き渡される文字列をパース（構文解析）することで、危険な値を分類し、判定を行える機構（セキュリティ判定部）の実装を行った。

その上で、スクリプト・インジェクション・アタックに対する脆弱性が知られているサーバサイド・アプリケーション（問題が修正される前のバージョン）を発掘し、実環境で脆弱性を再現できるように実行環境を構築し、セキュリティ判定部の実装を行った処理系が、実際の攻撃を検出可能であるか検証した。

研究開発目標	達成度
①定義体の文法の策定	①シンプルな定義体として、「クォート（' ）」内およびスペースの入らない数値等の値を対象として、実装し、評価したところ、それだけでもほぼ完全な検出を実現できることが判明した。達成度 100%
②コマンド解析部の実装・動作確認	②PHP-SWIFT 処理系を解析して、実際に組み込むポイントを見極め、SQL 文とその各文字の taint 情報を確認して SQL を確認する関数を追加した。達成度 100%
③攻撃検出機構の実装・動作確認	③PHP 処理系の解析を行い、MySQL に対する検出機構の実装を行った。達成度 100%
④実環境での脆弱性の再現	④WordPress 本体とそのプラグインの、SQL インジ

	ェクションに対する脆弱性を調査し、その中から果を示せる可能性のある脆弱性を 5 種類ほど実際に検証し、その中の 2 つの脆弱性を採用した。達成度 100%
⑤90%程度のオーバヘッド削減	⑤PHP-SWIFT の改良におけるボトルネック調査と連携して、結果的に無駄な処理となっている部分に対して改良を加えて速度向上の効果を検証した。達成度 100%
⑥実環境において攻撃の検出を確認	⑥④で構築した実環境において、攻撃により発生する一連 SQL のクエリの中に汚染されたデータが検出され、攻撃を停止した。さらに、動作が現実的な範囲の時間で収まることについても検証した。達成度 100%

②今後の展開

まず本研究開発成果の対外的アピールすること、並行してより具体的な応用イメージの提案と実証を行うこと、他の言語処理系や SQL インジェクション以外のインジェクション攻撃への対応といった拡大が必要と考える。

なにより、産学連携による新しい、セキュリティソリューションの市場への提案が重要である。これは、インジェクション攻撃が未だに収まるどころか、いつまでも深刻な問題であり、近年盛んに話題となる Web Application Firewall（WAF）のようなソリューションに対して、別アプローチを提案することのインパクトは大きい。

3. 総合所見

目標通りの成果が得られているが、イノベーション創出の可能性を見出すためには、さらなる研究開発が必要である。

SQL インジェクションアタックを対処療法的ではなく、普遍的に防御する手法として独自性があり、研究開発においても当初の目標はほぼ達成できた。今後は本手法の普及を考慮し、競合に対する優位性を主張できるだけの理論的な実証が求められる。