「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」
平成 20 年度採択研究代表者

平成 20 年度
実績報告

倉光　君郎

横浜国立大学　工学研究院　准教授

Security Weaver とＰスクリプトによる実行中の継続的な安全確保に関する研究

1. 研究実施の概要

本年度では、実行時のディペンダビリティを実現するための新しいオペレーティングシステムのサービスとして、早期警戒型ディペンダビリティモニタリングアーキテクチャ(EWDMA)を提案し、それに基づいて Security Weaver と P−スクリプト言語（ポリシー記述言語）の実装を行った。EWDMA の特徴は、PDCA サイクルの CHECK と ACT をモデル・ポリシー化し、適用領域ごとに異なるディペンダビリティへの要求を再構成可能にする点である。また、AO(Accounting Object)をサービスの単位として、モニタリングや制御を統一的にコントロールすることで、記述のしやすさと性能要求を満たしている。我々は、Security Weaver を LSM(Linux Security Module)の上に構築し、EWDMA モデルの上で動作可能なように、AO 単位のマルチセキュリティモデル化を実装し、アクセス制御時のパフォーマンス低下がほとんどないことを確認した。同時に、静的な型付きオブジェクト指向スクリプティング言語の高速化に取り組み、ポリシー記述言語としての拡張を行った。今後は、EWDMA の開発を進め、Konoha 言語をベースとしたディペンダビリティポリシー記述を実現する予定である。

2. 研究実施内容（文中にある参照番号は 4.(1)に対応する）

本年度では、実行時のディペンダビリティを実現するための新しいオペレーティングシステムのサービスとして、早期警戒型ディペンダビリティモニタリングアーキテクチャ(kernel-eye)を提案し、それに基づいて Security Weaver と P−スクリプト言語（ポリシー記述言語）の実装を進めた（図1）。

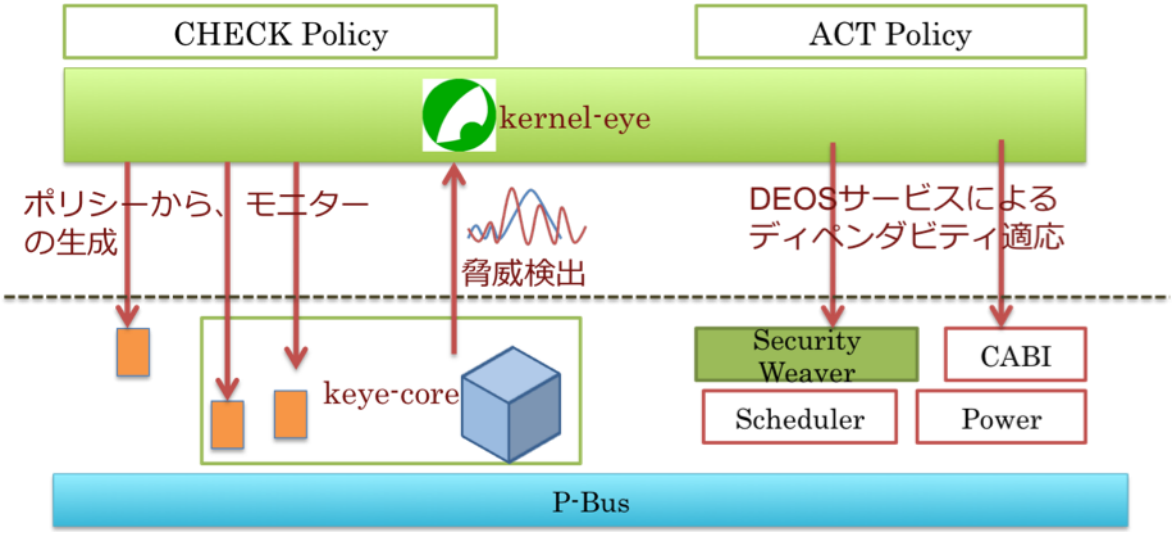

図1 Kernel-eye 早期警戒型モニタリングアーキテクチャ

EWDMA の特徴は、PDCA サイクルの CHECK と ACT をモデル・ポリシー化し、適用領域ごとに異なるディペンダビリティへの要求を再構成可能にする点である。また、AO(Accounting Object)をサービスの単位として、モニタリングや制御を統一的にコントロールすることで、記述のしやすさと性能要求を満たすことを目指している。

1） Security Weaver

Security Weaver は、実行時にアクセス制御ポリシーを埋め込むための機能である。我々は、Linux カーネルでは標準となっている上で、LSM(Linux Security Module)の上に Security Weaver 機能の実装(図2)を進めた。その結果、EWDMA モデルの上で動作可能なように、AO 単位で LSM 対応のセキュリティモデルを複数切り替えられるようになった。

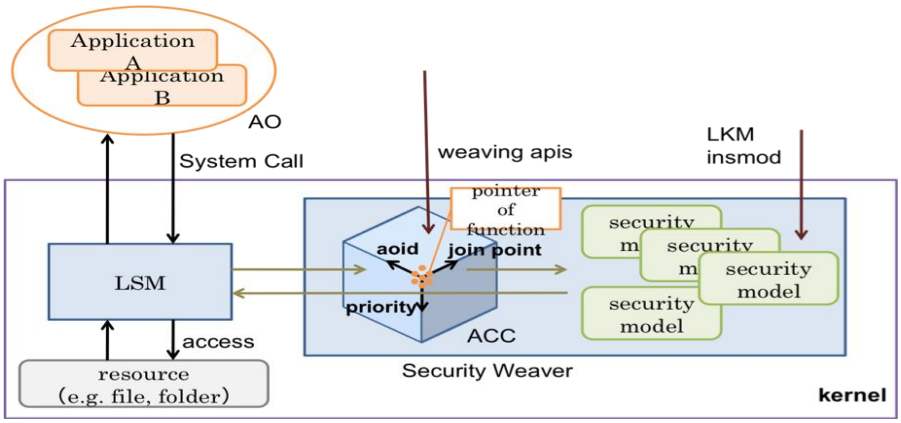

図2 Security Weaver の実装（LSM）

同時に、図3の通り、各種システムコールに対し、LSM と Security Weaver の両者の実行速度を比較し、アクセス制御時のパフォーマンス低下がほとんどないことを確認した。

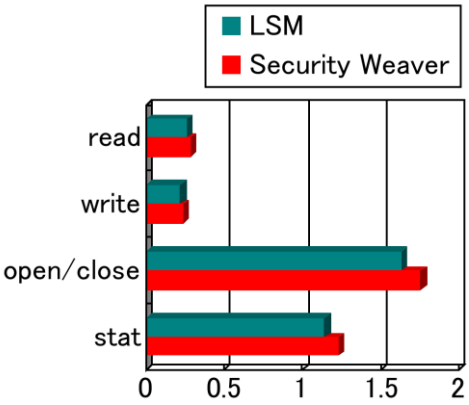

図3　Security Weaver の LSM に対するオーバーヘッド

2)　P-SCRIPT 言語の開発

我々は、ディペンダブルポリシーの記述言語として、静的な型付きオブジェクト指向スクリプティング言語である Konoha の開発を進め、複雑なポリシーの条件を高速に処理するため、その高速化に取り組んだ。既存のスクリプティング言語に対し、十分な高速化を実現したことが本年度の成果といえる(図4)。

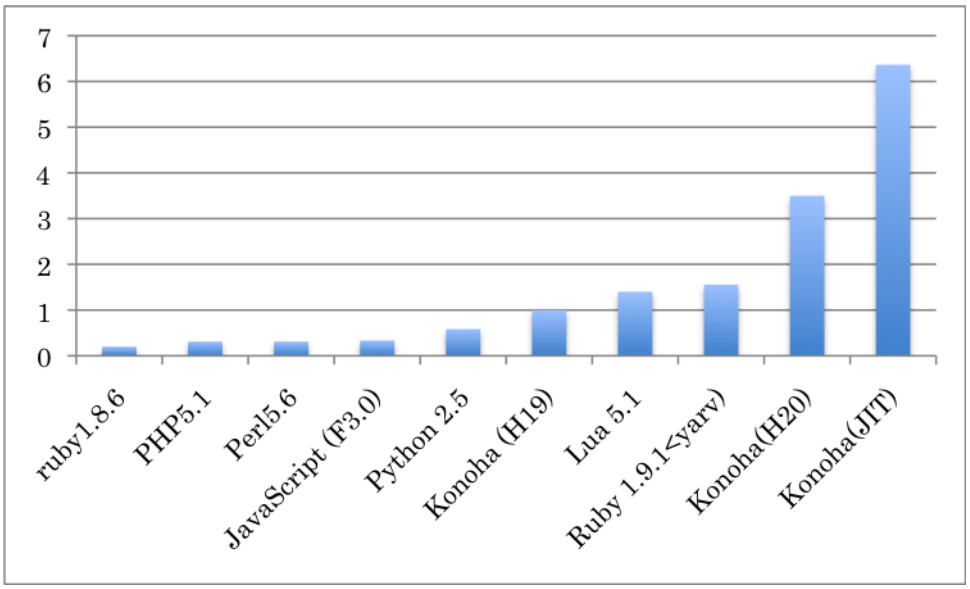

図４：　Konoha スクリプティング言語の速度比較

3. 研究実施体制

(1)倉光グループ

①研究分担グループ長:倉光　君郎(横浜国立大学、准教授)

②研究項目

（1） Security Weaver による実行時のセキュリティモデル切り換え

（2） P-Script によるディペンダビリティの記述

4. 研究成果の発表等

特許出願

平成 20 年度 国内特許出願件数：0 件（CREST 研究期間累積件数：0 件）