様式 C-7-2

自己評価報告書

平成２１年　４月３０日現在

研究種目：特定領域研究
研究期間：2006 年度～2010 年度
課題番号：18049027
研究課題名（和文）　情報爆発に対応する高度にスケーラブルでセキュアなソフトウェア構成・更新方式
研究課題名（英文）　Highly Scalable Software Security for Information Explosion Environments

研究代表者
柴山　悦哉
東京大学・情報基盤センター・教授
80162642

研究分野：計算機科学
科研費の分科・細目：情報学・ソフトウェア
キーワード：アスペクト指向，開発環境，ソフトウェア検証，テスト自動化，オーバーレイネットワーク，コンテンツ配信，Web アプリケーション

１．研究計画の概要

高度にスケーラブルな情報基盤を安全に構築・運用することを目的に，以下の 3 点に焦点を絞った研究を行う．
・高度にスケーラブルなアクセス制御基盤
・高度にスケーラブルかつ安全なホスティング基盤
・高度にスケーラブルかつ動的なアプリケーション更新基盤
また，この目的を達成するために，ソフトウェア検証，ソフトウェアテスト，実行時ミドルウェアの技術を組み合わせ，設計から運用にいたるソフトウェアライフサイクルを意識した研究開発を行なう．

２．研究の進捗状況

主に以下の 4 項目について研究を行った．

(1) スケーラブルなソフトウェアのための開発・更新環境:分散アスペクトの動的織り込み機構の設計，クラスタ上での実証実験などが完了した．技術的には，動的織り込みのタイミング制御を行うメタアスペクトを導入し，別の関心事として分離記述を可能とした点に大きな特徴がある．この技術は，動的なアプリケーション更新基盤の鍵となるだけでなく，テスト環境の自動設定，モニタリングコードの追加などにも利用できるので，アクセス制御基盤やホスティング基盤を実現する軽量の基本技術としても有望である．

(2) インターネットアプリケーションのためのテスト手法: Web アプリケーションや POP3 サーバなどを対象に，脆弱性をほぼ自動的に検出する技術を開発し，有効性に関する予備実験を完了した．攻撃用リクエストを生成するために，細粒度のテイント追跡と実行系からのフィードバックを用いる手法，アプリケーションのプロトコル定義を用いる手法などを検討し，有効性の検証は実アプリケーションを対象に行なった．

(3) 分散ハッシュテーブルの効率化: スケーラブルな情報共有のために，オーバーレイネットワークを用い，負荷変動に応じて自動的にレプリカの生成・削除を行う方式を提案し，シミュレーションによりその有効性を検証した．アンダーレイネットワークのトポロジーや遅延の動的な変化に対応し，仮想マシンを用いたサーバの自動的な配備なども行なっている．

(4) 表明記述のスケールアップ: アスペクト指向の考え方を導入することにより，スケーラブルな表明記述を可能とする方式について研究を行っている．プロトコルを表現する表明記述，履歴に依存した表明記述などを導入し，SourceForge で公開されているソフトウェアをサンプルとして仕様記述の事例研究を行った．

３．現在までの達成度

① 当初の計画以上に進展している。

この研究の目標を一言で述べると，情報基盤の安全性とスケーラビリティを両立させることである．そこで，安全性とスケーラビリティの両面から，現在までの達成度を自己評価する．

安全性に関して当初の計画で予定していたのは，ミドルウェア層での運用時対策技術を確立することであった．しかし，研究の進展にともない，ソフトウェアの設計段階とテスト段階の対策技術を組み合わせた方が望ましいことが判明した．その結果，当初の計画に比べ，より広範な対策技術の研究が進んだ．特に，アスペクト指向技術について，検証，テスト，運用の各段階で，それぞれ異なる重要な位置づけを見いだせた点は，当初想定していなかった成果である．

スケーラビリティに関して当初の計画で最初の 3 年間に達成を予定していたのは，数百～数千ノード規模の実験をシミュレーションにより行なうことであった．運用時技術に関しては，既に数千ノード規模のシミュレーション実験で有効性を確認しており，これはほぼ想定通りである．ただし，PlanetLab で取得した実データに基づく実験ができた点は当初の予定を上回っている．さらに当初の予定になかった開発時技術に関して，実機を用いた数十～100 ノード級の実験が完了している点も当初の予定を上回る成果である．

４．今後の研究の推進方策

最初の３年間で基礎的な方式の検討と予備実験の段階をほぼ終了したので，今後は，より高度なスケーラビリティを目指し，現実的な分散計算環境を意識した研究を進める予定である．

そのための実験用のメインのプラットフォームとしては，本領域の支援班が構築している分散計算環境 InTrigger を利用する．InTrigger の規模は年々大きくなっており，今後さらにスケールアップした実験が行なえると予想している．その他に，TSUBAME，T2K などのクラスタ型のスーパーコンピュータ，クラウドコンピューティング環境，PlanetLab などの利用も進める予定である．このように多様な実験環境を利用することで，特定の実験環境の問題が研究の妨げとなるリスクを軽減し，また研究成果の適用可能性の見積もりもより高い精度で行えるようになると考えている．

なお，クラウドについては，本研究課題が始まってから注目を集めるようになったものである．近未来の計算環境として有望であることは間違いなく，これを意識して研究を進める必要がある．しかし，この分野の変化は急激であり，研究者の間でもコンセンサスが取れていない部分も多いので，常に視野に入れつつ，必要に応じて計画変更を行なう方針である．

５． 代表的な研究成果

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１１件）

[1] Michihiro Horie, Shigeru Chiba, AspectScope An Outline Viewer for AspectJ Programs, Journal of Object Technolgoy, 査読有, Vol. 6, pp. 341-361, 2007.

{2} Kiyoshi Yamada, Takuo Watanabe, An Aspect-Oriented Approach to Modular Behavioral Specifications, Electronic Notes in Theoretical Computer Science, 査読有, Vol. 163, pp. 45-56, 2006.

〔学会発表〕（計４３件）

[1] Thanh-Binh Dao, Etsuya Shibayama, Automatic Security Testing for Web Applications, International Symposium on Engineering Secure Software and Systems, 2009.2.6, Leuven, Belgium.

[2] Yoshihisa Abe, Hiroshi Yamada, Kenji Kono, Enforcing Appropriate Process Execution for Exploiting Idle Resources from Outside Operating Systems, ACM European Conference on Computer Systems, 2008.4.2, Glasgow, Scotland.

[3] Hiroshi Yamada, Kenji Kono, FoxyTechnique: Tricking Operating System Policies with a Virtual Machine Monitor, ACM International Conference on Virtual Execution Environments, 2007.6.13,San Diego, USA.