平成 19 年度
実績報告

「情報社会を支える新しい高性能情報処理技術」
平成 15 年度採択研究代表者

加藤　和彦

筑波大学大学院システム情報工学研究科・教授

自律連合型基盤システムの構築

1. 研究実施の概要

膨大性、多様性、開放性を有する利用環境において、自律性と複合性を複合的に構成することができる情報基盤システムの設計原理の確立、同原理に基づいたシステム実装、およびその有効性の検証に関する研究を行う。統一的な設計原理として、仮想計算環境の原理について研究を行い、物理環境とは独立に自律性を有する仮想計算環境を構成し、さらに複数の仮想計算環境を連合させ、自律性を有する計算環境を構成可能とする。

本研究は、自律連合システム、仮想計算環境、データ・インターオペラビリティ、分散コンピューティングの言語と検証という四つの研究分野により構成されている。

自律連合システムに関する研究では、仮想計算機を高速転送する技術、自律した複数サイトが連合することによってインターネット上のサービス提供を持続可能するサステーナブルシステム、自律したサイト間のアクセス制御技術の開発を進めている。また、仮想ネットワークの制御や仮想インターネット実験プラットフォームの開発も行っている。

仮想計算環境に関する研究では、複数の計算機を連合させて利用するための仮想マシン技術、および OS のインタフェースを仮想化することにより軽量な仮想計算環境を実現する技術の開発を進めている。

データ・インターオペラビリティに関する研究では、オープン環境における情報源連合を目的とし、シームレスかつセキュアなデータ相互運用を実現するための情報統合基盤、ならびに知識発見・知識獲得を用いた情報源連合に関する研究開発を行っている。

分散コンピューティングの言語と検証に関する研究では、自律性を持つソフトウェアシステムが交換するデータの安全性や文法的妥当性を静的に検査する研究、および高度な論理推論や記号計算アルゴリズムを組み込んだ、複数の自律言語システムの連合によって構築されたシステムの開発を行っている。

2. 研究実施内容

自律連合システムグループは、以下の4点に関する研究を行った。第一に、昨年度までに開発したサステーナブルフレームワークの成果をもとに、複数サービスへの対応化や複数仮想機械への対応化を行った第二次基盤ソフトウェアの構築を行った。第二に、その際に複製プロトコルの信頼性や仮想機械の性能が問題となることから、これらの改良を行った。第三に、サーバの実行状態は仮想機械でカプセル化できる反面、アプリケーション・データの管理手法が問題となることから、インターネットサービスに適した分散データオブジェクトの設計やストレージの自動設定機構の開発を行った。第四に、自律性と連合性を実現するためのアクセス制御の手法として、ケーパビリティに基づく方式に着目し、オープンな環境上でアクセス制御を行う方式の開発を行った。

自律連合型基盤システムのための仮想ネットワーク環境に関する研究では、自律連合システムにおける情報流通および管理基盤の研究を行った。情報流通基盤として分散環境での効率良い処理スケジューリングや複製分散技術の研究を、情報処理基盤として情報の処理や蓄積を管理する技術や分散実行処理技術を展開した。分散で同期的に情報を蓄積・更新するためには、更新履歴を容易に追跡できることが重要であり、昨年度にログ構造化ファイルシステムを用いた分散同期複製技術を研究した。本年度は、これを支援する目的で、ログ構造化ファイルシステム上に保存された更新履歴を追跡管理するための管理システム「NILFS CPviwer」を作成した。また、分散複製上で処理を随意に移動させるために、JavaScript の実行状態を保存したままで遠隔に移動させる言語処理系を実現した。これらが連携することで分散環境での処理が実現されるが、さらにこの実行を外部から監視して異常などに対して安全性を維持する枠組みの研究を進めた。以上の情報処理基盤のなかで、実際にどのように処理を分散させるかについては、ヒューリスティックベースでネットワーク基盤から得られる状態の変動を学習しつつ処理を制御する技術の研究を行った。これにより、集中管理をせずに分散・自律的に処理の配置が可能となる。さらに、広域分散環境で情報の複製を効率良く配置するためのデータ転送手法として、リング状にパイプライン転送し短時間で多くのサイトに複製が配置される手法の評価を行った。

自律連合型基盤システムのための仮想計算環境に関する研究では、今年度は、安全な計算環境を実現するための仮想マシン技術および OS のインタフェースを仮想化することにより軽量な仮想計算環境を実現する技術の実装と実験に注力した。具体的には、第一に、仮想マシンの外側から仮想マシンの中の処理を監視・制御するシステムを設計・実装した。そのシステムは仮想マシン内の OS 上で実行されるシステムコールの動作をセキュリティポリシーによって制御できる。システムコールの動作を制御するセキュリティシステムは過去に多くあったが、それらと比べて本システムが独自であるのは、OS の内側からではなく外側から監視・制御を行う点である。これにより、攻撃者に乗っ取られたプログラムがセキュリティシステムを攻撃するのが極めて困難になっている。第二に、OS インタフェースの仮想化に関する技術を洗練させ、一つの OS 上に数千個の仮想的な計算環境を構築できるシステムを実装した。このシステムは、仮想計算環境のネットワーク接続のパターンおよび通信の様子を指定、視覚化する機能、テストやデバッグを効率化するための機能を含む。

実験では、数千個の仮想計算環境を作り、各環境を仮想的な計算機にみたてて P2P ソフトウェアを実行した。その結果、P2P ソフトウェアはその仮想計算環境上で十分に速く動作することが確認された。

自律連合型基盤システムのための自律的に起動可能なネットワーク OS に関する研究では、自律連合システムのOS起動法としてHTTPサーバからブロックデバイスイメージを取得する方式を開発／最適化した。平成18年度に作成したものはネットワークレイテンシが長い環境（海外サーバからの起動など）では極端にバンド幅が落ちることが判明していた。これを最適化するために、起動プロファイルによるディスクイメージの最適化手法(Ext2Optimizer)の適用や先行ダウンロードの方式(DLAHEAD: Download ahead)の改良を行った。また、OS 起動は通常の PC のみならず、仮想計算機上でも実行可能であることを確認した。現在のところ、Xen、QEMU、KVM で利用可能であることを確認した。

自律連合型基盤システムのための仮想ネットワークサブグループに関する研究では、平成19年度においては、これまでに実現した複数ノード上で大きな仮想IPネットワークトポロジを構築するための「仮想インターネットシステム」内において、「遅延」、「ジッタ」、「パケットロス」の3種類のネットワーク上の現象をシミュレーションする機能の実装に関する研究を行った。これらを仮想 IP ネットワーク内で生成する機能により、IP を用いる通信アプリケーションの開発・検証の際に、品質の不安定なインターネット上で開発中のアプリケーションが正しく動作するかどうかを検証することができるようになる。この研究で得られた知見に基づき、遅延・ジッタ・パケットロスの発生に関するパラメータをユーザが GUI から設定できるようにするための実装を進めている。また、仮想インターネットシステムの研究・実装によって得られた知見をもとに、「サステーナビリティを有するストリーム中継システム」の設計・実装を開始した。本研究は、拡張性と耐障害性に優れたデータストリーム中継システムとソケットAPIと互換性のある通信ライブラリの実現に関する研究である。このシステムは、中継ゲートウェイ、サーバおよびクライアントの三つのモジュールに分かれており、中継ゲートウェイはスケーラビリティを確保するため、負荷分散を実現する形で実装する。サーバおよびクライアントは、ソケットと同等の API を提供するライブラリとして実装する。これまでに通信ライブラリとゲートウェイシステムの設計・実装と筑波大学内へのテスト用ゲートウェイ（5ノード）の設置を行った。現在、本研究によって実装したライブラリを通信アプリケーションの開発者向けにインターネットで公開する準備を進めている。

データ・インターオペラビリティグループは、オープン環境における情報源連合を目的とし、シームレスかつセキュアなデータ相互運用を実現するための情報統合基盤、ならびに知識発見・知識獲得を用いた情報源連合に関する研究開発を行った。持続分散型情報統合基盤に関しては、基盤システム StreamSpinner と自律連合システムグループのサステーナブルシステムとの連携を強化するとともに、評価実験等により従来手法との比較検討を行った。我々の高信頼化方式は拡張性に優れており、利用者が独自のアプリケーション処理を組み込むような場合にも、それらを含めたデータ処理の持続性を保証できる。セキュア情報統合基盤では、各情報源のアクセス制御を考慮した情報統合のデモシステムを OGSA-DAI/DQP をベースとして実装した。P2P 型情報探索基盤

では、構造型 P2P ネットワークにおける XML データのキーワード検索を実現した。キーワード検索の効率的処理のために、分散ハッシュ表上に分散配置された転置リストを用いる問合せ処理方式を提案した。情報源からの知識抽出に関しては、例示レコード集合に基づく関連レコード抽出手法の評価実験を行い、抽出レコード数の増加、抽出精度の向上、処理コストの削減についての検証を行った。

広域ネットワーク環境グループでは、自律連合ネットワークサービスのための広域ネットワーク環境の構築の要件を定義し、インターネット上に展開された PlanetLab のような広域ネットワーク上のオーバーレイネットワークの実験環境において、サービスの実用化を目指した実証実験を行った。特に、広域ネットワークに起こり得るさまざまな障害に対して耐性を備え、高い可用性を実現するサステーナブルなサービスをインターネット上に展開し実用化するために必要とされる、広域ネットワーク環境構築のための要素技術の研究開発を行った。具体的には、(1)現在のインターネットの耐攻撃性(Robustness)を向上する要素技術の研究開発と、(2)ネットワークを(a)より効率的に利用し(効率性の向上)(b)より耐障害性をもつ(可用性の向上)ための要素技術の研究開発を行った。(1)では、分散 DoS 攻撃に耐えうるネットワークサービスを構築するために、オーバーレイネットワーク(ネットワーク仮想化)技術を応用し、コンピュータ資源が少なくても耐攻撃性を向上させるアーキテクチャ(Burrows, Overfort)を定義し研究開発を進めた。(2)では、現在のインターネットでは複数経路によるデータ配信ができないという制限があるが、これを解決するために新しい複数経路制御を、オーバーレイネットワークを用いて実現するアーキテクチャの研究開発(SORA)を進めた。

分散コンピューティングの言語と検証グループは、自律性を持つソフトウェアが交換する文字列データの安全性や文法的妥当性を静的に検査する研究を行っている。 前年度までに、プログラムが出力する文字列を静的に解析し、文脈自由文法を用いて近似するプログラム解析(文字列解析)を開発し、動的に生成されるXML文書の妥当性の検査を実現した。また、高度なウェブプログラミングを必要とするウェブ折り紙システムを開発し、ウェブプログラミングの問題点の分析を行っている。本年度には、主に以下の研究を行った。第一に、前年度までに開発した動的に生成される XML 文書の妥当性検査の手法を拡張し、HTML についての妥当性検査手法を開発した。第二に、文字列解析に基づいて、サーバサイドプログラムのクロスサイトスクリプティング脆弱性を検出する研究を行った。2007 年に Wassermann と Su により文字列解析と情報流解析を組み合わせて、SQL インジェクション脆弱性を検出する手法が提案された。しかし、クロスサイトスクリプティングでは、攻撃の形態がより複雑であり、単純にこの手法を適用しただけでは不十分である。本研究では、これまでに開発してきた妥当性技術とこの手法を組み合わせることで、クロスサイトスクリプティング脆弱性を検出する研究を行った。

3. 研究実施体制

(1)「自律連合システム」グループ

①研究者名:加藤　和彦（筑波大学）

②研究項目

・自律連合型分散システムの構築

(2)「ネットワーク環境」サブグループ

①研究者名:廣津　登志夫（豊橋技術科学大学）

②研究項目

・自律連合型基盤のためのネットワーク環境

(3)「セキュアな実行環境」サブグループ

①研究者名:大山　恵弘（電気通信大学）

②研究項目

・自律連合型基盤のための仮想計算環境

(4)「自律的に起動可能なネットワーク OS」サブグループ

①研究者名:須崎　有康（産業技術総合研究所）

②研究項目

・Internet からの OS 起動に関する研究

(5)「仮想インターネット」サブグループ

①研究者名:登　大遊（ソフトイーサ株式会社/筑波大学）

②研究項目

・仮想インターネットの設計と実装

(6)「データ・インターオペラビリティ」グループ

①研究者名:北川　博之（筑波大学）

②研究項目

・自律連合型基盤のためのデータ・インターオペラビリティと自律連合型情報システム

(7)「広域ネットワーク環境」グループ

①研究者名:中尾　彰宏（東京大学）

②研究項目

・自律連合型基盤のための広域ネットワーク環境の構築

(8)「分散コンピューティングの言語と検証」グループ

①研究者名:井田　哲雄（筑波大学）

②研究項目

・Web プログラミングのモデル化、スクリプト言語のプログラム解析

4. 研究成果の発表等

(1) 論文発表(原著論文)

1. Mizuki Oka and Kazuhiko Kato, “Anomaly Detection Using Integration Model of Vector Space and Network Representation”, IPSJ Journal, Vol.48, No.6, pp.2118-2128, 2007.
2. Akiyoshi Sugiki, Kei Yamatozaki, Richard Potter, Kazuhiko Kato, “A Platform for Cooperative Server Backups based on Virtual Machines”, International Service Availability Symposium 2008, LNCS, 2008 （採択済み, 2008 年 5 月掲載予定).
3. Mitsuhiro Mabuchi, Yasushi Shinjo, Akira Sato, and Kazuhiko Kato, “An Access Control Model for Web-Services that Supports Delegation and Creation of Authority”, The 7th International Conference on Networking (ICN'08), 2008 (採択済み, 2008 年 4 月掲載予定)
4. 川崎仁嗣, 阿部洋丈, 加藤和彦, “プロセストレース機構の多重化法”, 情報処理学会論文誌:コンピューティングシステム, 2008 年(採択済み, 2008 年掲載予定).
5. Koichi Onoue, Yoshihiro Oyama and Akinori Yonezawa, “Control of System Calls from Outside of Virtual Machines”, In Proc. of the 23rd Annual ACM Symposium on Applied Computing (SAC 2008), Ceara, Brazil, pp. 2120-2125, March 2008.
6. Tomohiro Shioya, Yoshihiro Oyama and Hideya Iwasaki, “A Sandbox with Dynamic Policy Based on Execution Contexts of Applications, In Proc. of the 12th Annual Asian Computing Science Conference (ASIAN '07), Vol. 4846 of LNCS, Doha, Qatar, pp. 297-311, December 2007.
7. Jianwei Zhang, Yoshiharu Ishikawa and Hiroyuki Kitagawa, “Record Extraction Based on User Feedback and Document Selection”, In Proc. of Joint Conference of 9th Asia-Pacific Web Conference and 8th International Conference on Web-Age Information Management (APWeb/WAIM 2007), LNCS 4505, pp. 574-585, HuangShan, China, June 2007.
8. Toshiyuki Amagasa, Chunhui Wu and Hiroyuki Kitagawa, “Retrieving Arbitrary XML Fragments from Structured Peer-to-Peer Networks”, In Proc. of Joint Conference of 9th Asia-Pacific Web Conference and 8th International Conference on Web-Age Information Management (APWeb/WAIM 2007), LNCS 4505, pp. 317-328, HuangShan, China, June 2007.
9. Yousuke Watanabe, Shinichi Yamada, Hiroyuki Kitagawa and Toshiyuki Amagasa,

"Integrating a Stream Processing Engine and Databases for Persistent Streaming Data Management", In Proc. of 18th Int'l Conference on Database and Expert Systems Applications (DEXA2007), Regensburg, Germany, LNCS 4653, pp. 414-423, Sept. 2007.

10. 呉俊輝, 天笠俊之, 北川博之, "構造型 P2P ネットワークにおける負荷分散を考慮した XML データ処理", 日本データベース学会 Letters, Vol. 6, No. 1, pp. 93-96, 2007 年 6 月.
11. 山田真一, 渡辺陽介, 北川博之, 天笠俊之, "データストリーム管理システム Harmonica の設計と実装", 情報処理学会論文誌:データベース, Vol. 48, No. SIG14 (TOD35), pp. 91-106, 2007 年 9 月.
12. 渡辺陽介, 北川博之, "分散ストリーム処理環境における持続型問合せ処理方式", 日本データベース学会 Letters, Vol. 6, No. 2, pp. 41-44, 2007 年 9 月.
13. 渡辺陽介, 秋山亮, 大喜恒甫, 北川博之, "映像ストリームのための映像情報統合基盤システムの提案", 日本データベース学会 Letters, Vol. 6, No.4. pp.13-16, 2008 年 3 月.
14. Tetsuo Ida, Hidekazu Takahashi, Mircea Marin and Fadoua Ghourabi, "Modeling Origami for Computational Construction and Beyond", In Proc. of the International Conference on Computational Science and Its Applications, LNCS 4706, pp.653-665, 2007.
15. Yasuhiko Minamide, "Verified Decision Procedures on Context-Free Grammars", In Proc. of the 20th International Conference on Theorem Proving in Higher Order Logics, LNCS 4732, pp. 173-188, 2007.
16. Asem Kasem and Tetsuo Ida, "Computational origami environment on the web", Frontiers of Computer Science in China, 2(1), pp. 39-54, 2008.
17. 松本宗太郎, 南出靖彦, "多相レコード型に基づく Ruby プログラムの型推論",情報処理学会論文誌:プログラミング, Vol.49, No. SIG 3, PRO 36, pp.39-54, 2008 年.
18. Soon Hin Khor, Nicolas Christin, Tina Wong and Akihiro Nakao, "Power to the People: Security the Internet One Edge at a Time", ACM SIGCOMM 2007 Workshop on Large-Scale Attack Defense (LSAD), 2007.
19. Soon Hin Khor and Akihiro Nakao , "Overfort: Combating DDoS with Peer-to-peer DDoS Puzzle",The 4th International Workshop on Security in Systems and Networks (SSN 2008), 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS 2008) (採録決定, 2008 年 4 月掲載予定).

(2) 特許出願

平成 19 年度 国内特許出願件数:0 件(CREST 研究期間累積件数:2 件)