「情報社会を支える新しい高性能情報処理技術」
平成 14 年度採択研究代表者

坂井　修一

（東京大学大学院情報理工学系研究科　教授）

「ディペンダブル情報処理基盤」

1．研究実施の概要

コンピュータとインターネットを中心とする情報システムが重要な社会基盤のひとつとなるにつれ、そのディペンダビリティ(dependability) の確保が大きな課題となっている。ディペンダビリティは、信頼性・安全性・可用性・堅牢性・拡張性などの複合的・総合的な性質である。今の情報処理環境は、アドホックにできあがっている部分が大きく、真にディペンダブルなシステムを形成しているとは言い難い。本研究では、超分散型情報処理環境に必須なディペンダビリティを高度に実現する情報処理基盤を研究開発する。特徴は、(1)アーキテクチャ・ソフトウェアのそれぞれでディペンダビリティ向上の要素技術開発を行うとともに、情報インフラ全体にわたる基盤技術の確立をめざす点、(2)再構成による安全性確保、メモリ操作高信頼化、効率と安全性を高度に高めた暗号処理、サーバの高信頼なスケジューリングなど、アーキテクチャや基礎ソフトウェアの新技術をディペンダビリティの基本要素としている点、(3)ディペンダビリティ向上のための基本要素をミドルウェアが呼び出す方式によってプログラマとディペンダビリティ管理者の役割を分け、全体として手数少なく確実にディペンダビリティを向上するようにできる点、(4)高いディペンダビリティ実現のためのカスタマイゼーションを安全確実に小さな手間で行えるようにする点、(5)クラスタサーバにおいて、ライブラリおよび実行時システム群の体系的な開発によって、高度なディペンダビリティの実現をめざす点、(6)ネットワーク侵入防止のために、イベント分析型の侵入検知システムを提案・試作・実証する点、などである。

本研究によって、ユーザが真に信頼でき、安全性・性能・機能の諸点でも満足できる情報システムの技術基盤が作られると考えられる。これが確立すれば、商取引や行政などの電子化が一気に進み、信頼性と利便性のともに高い社会をより低いコストで実現できるようになる。政府の提唱する IT 国家実現には必須のことであり、医療ネットワーク、防災ネットワーク、遠隔教育ネットワークなどの実現にも必要な技術となる。また、真にディペンダブルなハードウェア・ソフトウェアの創出は、産業的には、従来のインテル／マイクロソフトの次世代のヘゲモニーを狙う可能性を秘めている。特に、利潤構造を示しにくい現在の半導体産業を活性化するひとつの軸となることが期待される。

現状と展望を以下に簡単にまとめる。

本研究プロジェクトでは、前年度までで、アーキテクチャ、侵入検知システム、アプリケーション用

基盤ソフトウェア、サーバ用基盤ソフトウェアのそれぞれで新規性の高い要素技術の提案・実装・評価・検証を行い、それぞれ学会・国際会議などで発表して好評を博し、また、特許申請を行った。さらに前年度は、統合システムとしての超ディペンダブル CPU の研究と基本設計、超ディペンダブルサーバのシステム技術の開発を行い、侵入検知システムおよび河川水量監視システムのデモを行った。平成 18 年度は、超ディペンダブル CPU テストベッドの試作を行い、侵入検知システムの改良版製作、アプリケーション基盤ソフトウェアの最適化、サーバ用基盤ソフトウェアの改良（フラッシュクラウド対策など）を行った。最終年度は、超ディペンダブル CPU テストベッドの完成、試作した基盤ソフトウェア最適化、新しい WWW アプリケーションのデモンストレーションなどとともに、これまで以上に広範な技術統合を進めて、システムとしてのディペンダブル情報処理基盤の検証を行う。

2. 研究実施内容

平成 18 年度は、前年度までで開発・評価・検証した要素技術を最適化し、検討してきた統合技術の実現に向けての研究開発を進めた。また、全体の統合イメージを確定させるために、引き続き、数ヶ月に一度程度会合をもち、ここで研究の進捗や最新の成果についての情報交換をグループ間で行うとともに、研究ポリシーの確認、重点テーマの選択、デモのやりかたの検討などを行った。

以下に、各グループの平成 18 年度の具体的な実施内容と統合化の現状を記す。

アーキテクチャ研究グループでは、「エラー対策技術」、「タンパ対策技術」、「プログラム監視技術」を三本柱とし、効率的に統合実装する超ディペンダブル・プロセッサの開発を進めた。情報漏洩の防止やシステムの脆弱性対策など、従来は個別の事象毎のアドホックな対策が必要とされていたが、超ディペンダブル・プロセッサでは、三本柱の技術の連携により、構造的に安全な枠組みを提供する。

各要素技術について、エラー対策技術では、タイミング・エラーからの回復アーキテクチャの検討を行い、実証に向けたHDL 実装を開始した。本年度はベースラインとなるスーパスカラ・プロセッサを記述し、FPGA 上に実装した。記述したプロセッサは、複数命令の同時実行、アウト・オブ・オーダ実行、投機実行など、スーパスカラアーキテクチャに本質的な要素を備えており、ALPHA AXP 命令セットのサブセットを実行することができる。

タンパ対策技術では、「耐ソフトウェアタンパ・プロセッサ」を提案した。提案したプロセッサは rootkit 等に代表される、ソフトウェアによるタンパを、従来のセキュア・プロセッサよりも少ないオーバヘッドで防ぐことができる。

ハードウェア再構成技術を用いた故障に強い CPU のアーキテクチャについては、回路分割に基づく故障復帰方式について検討を行った。この方式では小規模のサブブロックを再構成可能な結合網で接続したロジックを用いて目的の機能を実現することで耐故障性を持たせる。また、CPU の実行ステージに特化した耐故障ロジックの構成について実行性能と電力の評価を行った。この方式では遅延とコストが異なる複数の演算器を結合網で接続したロジックを用いる。

プログラム監視技術では、プログラム挙動を把握するためのコア技術である、情報フロー追跡技術を提案した。また、セマンティックにプログラムの脆弱性を検出するコンパイラ技術について、検討を行った。

全体アーキテクチャでは、「タグ」を効率的に管理するハードウェア機構について提案、評価を行った。「タグ」はプロセッサがデータに動的に付加、伝播するもので、超ディペンダブル・プロセッサが実装する多くの要素技術で前提となっている。「タグ」はデータの安全性や権利関係、完全性等を命令レベルで追跡するために用いられる。

全体のシステムアーキテクチャについて、その構成を詳細化・具体化（図1）し、テストベッドを試作した。平成 19 年度に、テストベッド上での実装・検証を行う。

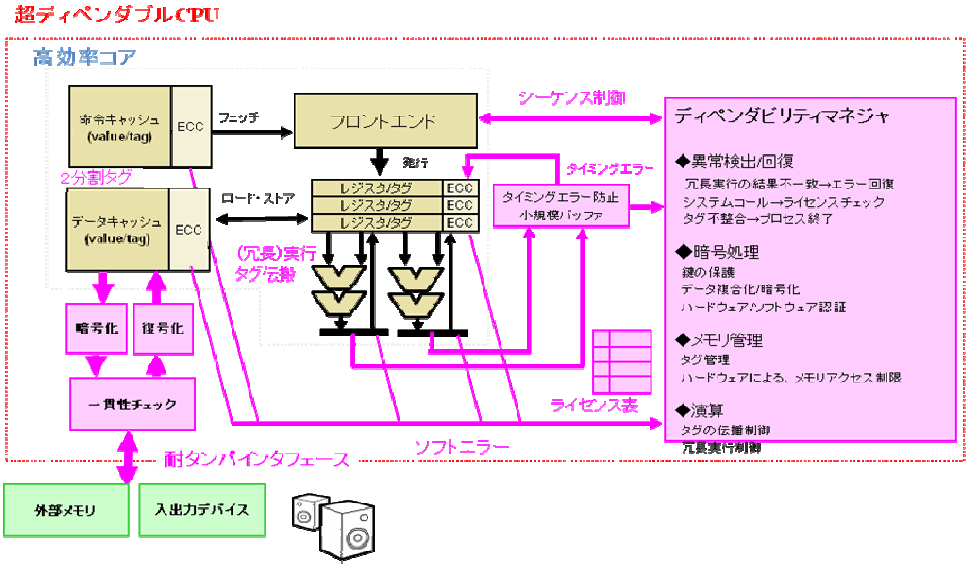

図1. 超ディペンダブル CPU の構成

侵入検知システム（IDS）については、前年度から引き続き、侵入パケットのパターンの学習による誤検出率の低減のやりかたを詳細化した。また、検査できる範囲を拡大するため、高速なバックボーンネットワークに直接接続して多数のトラフィックを検査可能な TCP ストリームのパターン照合方式を提案した。今年度は、TCP ストリームレベルでの情報を用いた高度な過負荷攻撃検出・抑制を中間ノードで実施するための方式を検討した。この方式では過負荷時の ACK パケットの振る舞いの異常に着目し、中間ノードで個々のストリームの状態を管理することにより攻撃を検出する。これら諸技術は新しいIDS基板の上で実装され、検証中である。

アプリケーション用基盤ソフトウェア研究グループでは、アスペクト指向技術を応用してディペンダビリティ機能を自動的にプログラム中に埋め込む技術を開発している。昨年度はこれまでの成果をまとめる形で web アプリケーション向けにアスペクト指向システム GluonJ を開発し、これを利用したデモ・アプリケーションを試作した。本年度は、このデモ・アプリケーションで使われているアス

ペクト指向・ディペンダブル技術をさらに洗練し、論文としてまとめた。このデモ・アプリケーションは河川の水位をインターネット経由で配信するweb アプリケーションである。ディペンダブルにするには混雑時にも河川の水位をセンサーから最優先で取得するようにしなければならないが、Java 言語等で開発された一般的な web アプリケーションではそのようなスケジューリングは困難である。OS はスケジューリング機能を提供するが、分厚いミドルウェア層が介在するため、OS のもつスケジューリング機能を、うまくアプリケーションのレベルの処理のスケジューリングに対応づけられないからである。我々はアスペクト指向システムを利用して、アプリケーションレベルでスケジューリングを実現するコードを対象のアプリケーションに自動挿入し、自動的にディペンダブルにする技術を、河川の水位を配信する web アプリケーションを例に開発した。この技術開発について報告した論文は、アスペクト指向分野の国際会議としては最もレベルが高いといわれるAOSD で発表し、高い評価を得た。また今年度は、さらなるディペンダビリティ技術を開発するため、そのテストベッドとしてのアプリケーション開発を始めた。

サーバ用基盤ソフトウェア研究グループでは、クラスタサーバを仮想的な高信頼計算機として抽象化するソフトウェア・レイヤの設計・開発を進めている。特に、サーバ・ソフトウェアの管理コストの低減を目指し、サーバの挙動を定める性能パラメータの自動調整機構の研究・開発を進めてきた。ウェブサーバの主要パラメータに特化した手法について、一定の研究成果を出し雑誌論文への投稿などを行った。この成果を踏まえ、より汎用性の高い自動調整手法の確立を目指し、サーバ・ソフトウェアの不安定状態を検出する機構についての研究を行った。本手法は品質管理工学の手法を応用し、サーバの不安定状態を品質の悪化として統計的に捕捉することを目指している。まだ汎用的な手法として確立するところまでは進んでいないものの、ウェブプロキシの性能劣化を捉えるなど少しずつ成果が出はじめている。また、フラッシュクラウドに耐性のあるサーバ管理基盤ExaPeer の開発も行った。なお、TCP/IP ストリームフィルタというネットワーク侵入防止システムについては、侵入防止のためのルールの記述力の向上やネットワーク侵入検知システムへの応用などを行い、従来手法よりフォールスポジティブが減少することを確認した。

以上、各グループの成果をふまえ、本プロジェクト後半の目標を定め、全体の統合イメージを作っている。具体的には、各要素技術と、これを使うミドルウェア技術の統合を、図2のように行うこととなる。

現在、最終統合デモシステムの具体化を進めている。これは、今のところ次のようなものになる予定である。

1. 超ディペンダブル CPU システムの詳細レベルシミュレータ。
2. 超ディペンダブル CPU テストベッド（第2版）： FPGA を核とした基板の実装により、ディペンダビリティの実装と評価検証を行う。

3. 超高速侵入検知ハードウェアの実装と最終デモ。
4. クラスタサーバ上の、サーバ用基盤ソフトウェアとアプリケーション用基盤ソフトウェアの統合。特に両者の協調動作によるサーバ安定化・安全化。
5. サーバのデモの拡充： 河川水量監視に加えてテレビ SNS。
6. クラスタサーバと IDS ハードウェアの統合。特に、TCP/IP ストリームフィルタ、IDS ハードウェア、侵入パターン学習の協調動作による高い検出率・低い誤検出率の実現。

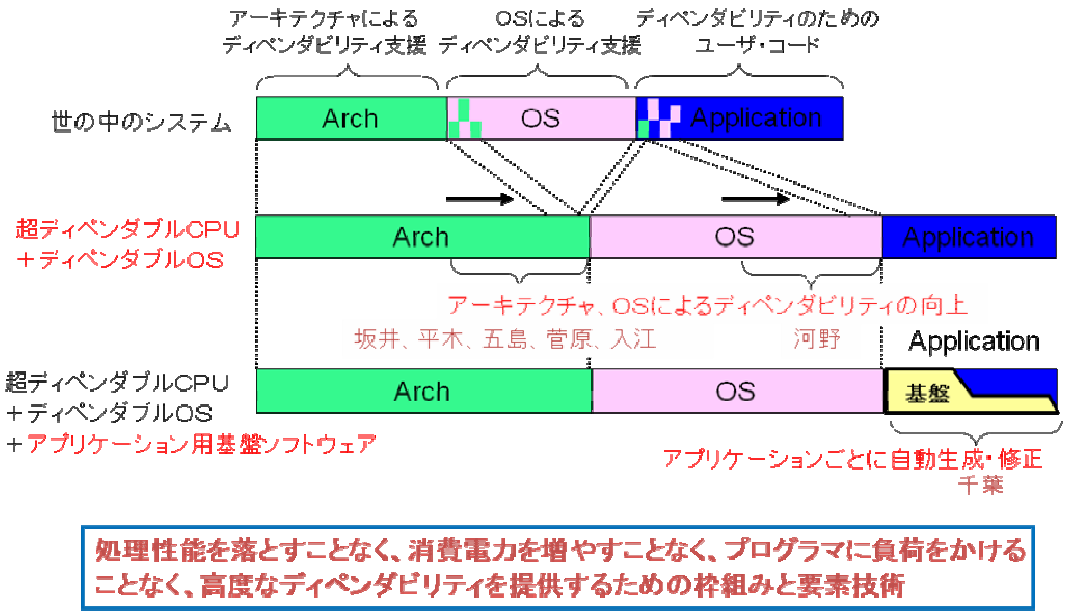

図2. 本プロジェクトの統合イメージ

3. 研究実施体制

(1)「アーキテクチャ研究」グループ

①研究者名

坂井　修一（東京大学大学院情報理工学系研究科電子情報学専攻　教授）

②研究項目

・再構成ハードウェアを用いた耐故障プロセッサ
・FPGA を用いた超高速侵入検知ハードウェア
・過渡故障を検出・回復するプロセッサ
・プログラム挙動を監視し、データの機密性を保護するプロセッサ
・ディペンダブル・プロセッサ要素技術を高効率に統合するアーキテクチャ
・統合アーキテクチャ

(2)「アプリケーション用基盤ソフトウェア研究」グループ

①研究者名

千葉　滋（東京工業大学情報理工学研究科　助教授）

②研究項目

・ディペンダブルなソフトウェア開発基盤の開発、

・アスペクト指向にもとづくプログラム変換ツールの開発、

・応用システムの開発

(3)「サーバ用基盤ソフトウェア研究」グループ

①研究者名

河野　健二（慶應義塾大学理工学部情報工学科　助教授）

②研究項目

・障害検出のための汎用的な手法の検討

・フラッシュクラウドに耐性のあるサーバ管理機構

・レイヤ 7 プロトコルの文脈を利用したネットワーク侵入検知

4. 研究成果の発表等

(1)論文発表（原著論文）

■国内学会論文誌

○Luong D. Hung and Shuichi Sakai: "Dynamic Estimation of Task Level Parallelism with Operating System Support", 情報処理学会論文誌コンピューティングシステム(ACS 14), Vol.47, No.SIG7, pp.43-51, May, 2006.

○松沼正浩、光来健一、日比野秀章、佐藤 芳樹、千葉 滋："過負荷時の Web アプリケーションの性能劣化を改善する Session-level Queue Scheduling"、コンピュータソフトウェア、vol.23、no.2、日本ソフトウェア科学会、2006、pp.199-210.

○三輪 忍, 福山 智久, 嶋田 創, 五島 正裕, 中島 康彦, 森 眞一郎, 富田 眞治: "パス情報を用いた分岐フィルタ機構", 情報処理学会論文誌コンピューティングシステム(ACS 15), Vol.47, No.SIG12, pp.108-118, Aug, 2006.

○Luong D. Hung, Masahiro Goshima and Shuichi Sakai: "Zigzag-HVP: A Cost-effective Technique to Mitigate Soft Errors in Caches with Word-based Access", 情報処理学会論文誌コンピューティングシステム(ACS 16), Vol.47, No.SIG18, pp.44-54, Oct, 2006.

○塩谷 亮太, ルォン ディン フォン, 入江 英嗣, 五島 正裕, 坂井 修一: "マルチコア・プロセッサの不均質共有キャッシュにおけるLRU 大域置き換えアルゴリズム", 情報処理学会論文誌コンピューティングシステム(ACS 17), Vol.48, No.SIG3, pp.59-74, Feb, 2007.

○杉木 章義, 河野 健二, 岩崎 英哉："リクエスト待機間隔を考慮したウェブサーバの keep-alive

時間の自動設定”, コンピュータソフトウェア, 掲載予定.

○阿部 勝幸, 岩崎 英哉, 河野 健二:”アプリケーション層プロトコルの記述に基づく拡張性に優れたプロトコル処理コード生成系”, コンピュータソフトウェア, 掲載予定.

■国際会議(査読付・年次論文集有)

○ Yoshisato Yanagisawa, Kenichi Kourai, Shigeru Chiba and Rei Ishikawa: ″A Dynamic Aspect-oriented System for OS Kernels″, Proc. of 5th Int'l Conf. on Generative Programming and Component Engineering (GPCE '06), 2006, pp.69-78.

○Hiroshi Yamada, Kenji Kono: “User-level disk-bandwidth control for resource-borrowing network applications”, In Proc. of IEEE/IFIP Network Operations and Management Symposium, CD-ROM, April, 2006.

○Makoto Shimamura, Kenji Kono:”Using Attack Information to Reduce False Positives in Network IDS”, In Proc. of IEEE Int'l Symp. on Computers and Communications, pp. 386-393, June, 2006.

○ Luong Dinh Hung, Masahiro Goshima and Shuichi Sakai: ″SEVA: A Soft-Error- and Variation-Aware Cache Architecture″, IEEE International Symposium on Pacific Rim Dependable Computing (PRDC 2006), Riverside, California, USA, pp.47-54, Dec, 2006.

○Satoshi Katsunuma, Hiroyuki Kurita, Ryota Shioya, Kazuto Shimizu, Hidetsugu Irie, Masahiro Goshima, and Shuichi Sakai: ″Base Address Recognition with Data Flow Tracking for Injection Attack Detection″, IEEE International Symposium on Pacific Rim Dependable Computing (PRDC 2006), Riverside, California, USA, pp.165-172, Dec, 2006.

○ Kenichi Kourai, Hideaki Hibino, and Shigeru Chiba: ″Aspect-oriented Application-level Scheduling for J2EE Servers″, Proc. of the 6th International Conference on Aspect-Oriented Software Development (AOSD '07), ACM Press, 2007, pp.1-13.

○Hiroshi Yamada, Kenji Kono: FoxyTechnique: Tricking Operating System Policies with a Virtual Machine Monitor, In Proc. of ACM Int'l Conf. on Virtual Execution Environments, To appear.

○Miyuki Hanaoka, Kenji Kono, Makoto Shimamura, Satoshi Yamaguchi: An Efficient TCP Reassembler Mechanism for Layer7-aware Network Intrusion Detection/Prevention Systems, In Proc. of IEEE Int'l Symp. on Computers and Communications, To appear.

(2)特許出願

H18 年度特許出願:1件(CREST 研究期間累積件数:3件)