「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によって、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がなされ、それぞれが学会・国際会議などで発表され、また特許申請などを行った。平成１７年度は、要素技術の実装・評価を進めるとともに、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。今後は、統合技術を完成させてシステムとしてのディペンダブル情報処理基盤を明らかにするとともに、サーバ用のデモの拡充などを行う。

２．研究実施内容

平成１７年度は、前年度までで開発した要素技術を発展・実装・検証するとともに、統合技術に向けてのシミュレータの実装や実アプリケーションの実装を進め、侵入検知システムと河川水量監視システムのデモを行った。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１７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、超ディペンダブルプロセッサが備えるべきディペンダビリティ機能を、“エラー耐性”、“タンパ耐性”、“プログラム監視”の三系統に整理し、それぞれについて要素技術の提案、評価を行った。エラー耐性技術では、従来から行われているソフトエラー対策技術に加え、製造ばらつきによる安全マージン減少への対策技術として、RAM への書き込み保証アーキテクチャを提案した。タンパ耐性技術では、前年度にひきつづき、外部バスを暗号化するアーキテクチャの研究を行った。プログラム監視技術では、バグや悪意を含むプログラム運用から、プロセス完全性を保護する技術、データ機密性を保護する技術それぞれについて、提案、最適化と評価を行った。さらに、これらの要素技術を統合するためのアーキテクチャ構成と性能オーバヘッド傾向について検討を行った。

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、故障検出についてのプログラム作成とＦＰＧＡ上で演算部位における回路性能の予備評価を行った。これは、実装時における各種パラメータを評価するためである。検出プログラムはターゲットアーキテクチャ専用にＣ言語により記述されている。再構成時の回路分割評価（回路性能評価）はＦＰＧＡ上における評価を行っており、さらに改良を進める予定である。

これら要素技術を統合するシステムアーキテクチャについて、その構成を詳細化した（図１）。平成１８年度以後に、統合化が進められる。

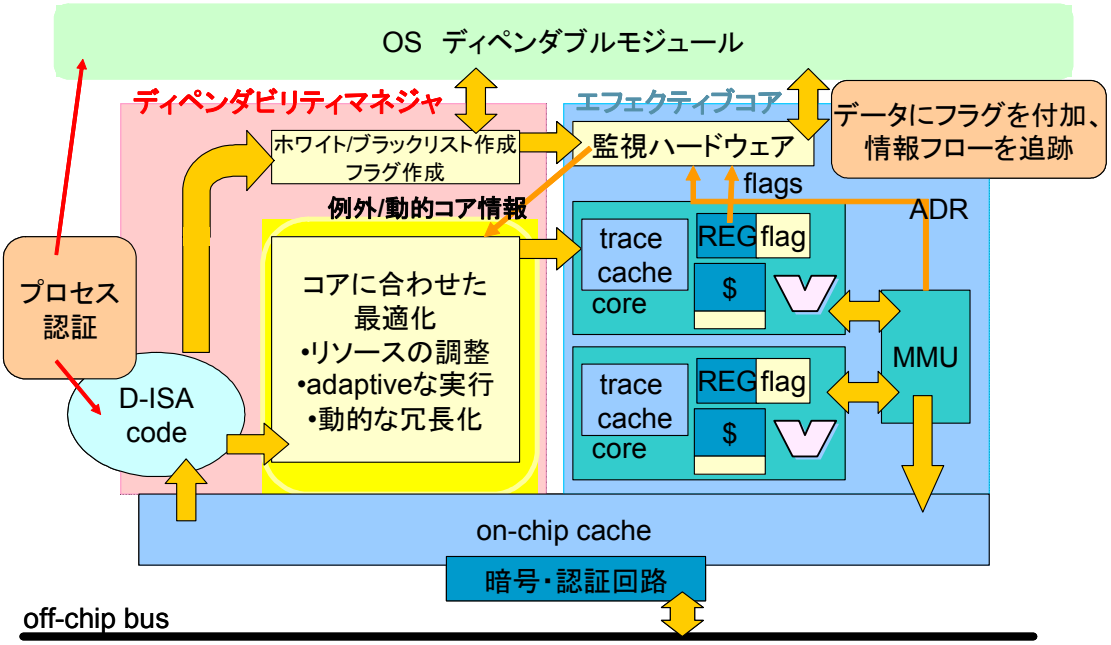


図１．超ディペンダブル CPU チップの構成

侵入検知システム（ＩＤＳ）については、前年度までの成果を受けて、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．この方式では，FPGA を使用して多数の TCP ストリームを少ないメモリ量で高速に検査する事が可能である．パケットを到着順に処理する事によりバッファリング量を抑える到着順照合法(逆順照合法)と，不正な再送パケットの存在下で照合結果の正しさを保証するパケットフィンガープリント法が主な提案点である．また，提案方式と前年度に提案した SBT 法を用いて，FPGA を搭載したネットワーク実験装置に TCP ストリームレベルの IDS を実装した．この IDS については平成 17 年末の CREST シンポジウムにおいてデモを行った．来年度は TCP ストリームレベルの情報を用いた高度な過負荷検出・抑制機構を確立し，過負荷という問題に対しても多数のトラフィックを同時に扱える事を可能にすることを目指す．

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。本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。この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

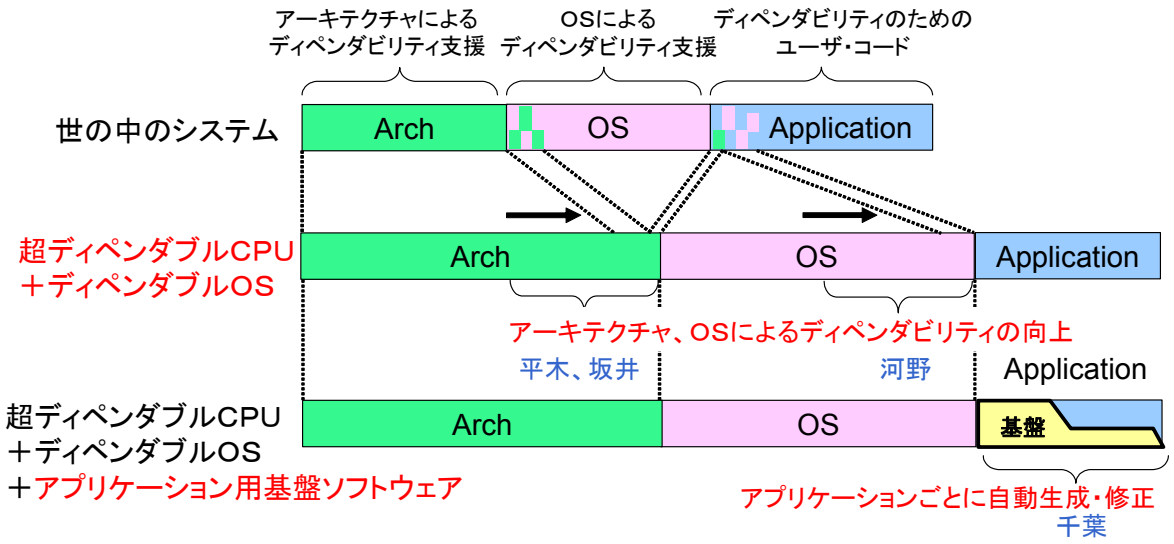
ルウェア層が介在するため、OS のもつスケジューリング機能を、うまくアプリケーションのレベルの処理のスケジューリングに対応づけられないからである。我々はアスペクト指向システムを利用して、アプリケーションレベルでスケジューリングを実現するコードを対象のアプリケーションに自動挿入し、自動的にディペンダブルにする技術を、河川の水位を配信する web アプリケーションを例に開発した。

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。昨年度に引き続き、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・開発を進めた。昨年度と同様にウェブサーバを対象とし、最大接続数というパラメータの自動調整機構を実現した。この自動調整機構は、昨年度の成果と組み合わせて利用することができ、ウェブサーバの主要パラメータの自動調整に成功したといえる。これまでの研究成果はウェブサーバのみを対象としていたが、来年度以降は、より汎用性の高い自動調整手法の確立を目指す。また、この研究と並行して進めている 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、その有用性を示すための実証実験を行った。2 週間以上に渡って収集した現実のメッセージ・ログを用いて、zero-day attack のような未知の攻撃に対しても十分な耐性を有することが確認できた。

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。

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 の一部 FPGA 化
３．　超高速侵入検知ハードウェアの実装とデモ
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、オンラインショップ、教育など
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。



アプリケーションプログラマに負荷をかけることなく、必要なディペンダビリティを提供する

図２．本プロジェクトの統合イメージ

３．研究実施体制

アーキテクチャ研究グループ（坂井修一）

①研究分担グループ長：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

アプリケーション用基盤ソフトウェア研究グループ（千葉　滋）

①研究分担グループ長：千葉　滋（東京工業大学大学院情報理工学研究科　数理・計算科学専攻、助教授）

②研究項目：

- アプリケーション用基盤ソフトウェアのためのアスペクト指向システムの研究開発
- 河川水位監視デモシステムのディペンダブル化技術の開発

サーバ用基盤ソフトウェア研究グループ　（河野健二）

①研究分担グループ長：河野　健二（慶応義塾大学理工学部情報工学科、助教授）

②研究項目：

- ウェブサーバを対象とした性能パラメータの自動調整機構
- 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防止システム

４．主な研究成果の発表（論文発表および特許出願）

（１）　論文（原著論文）発表

○ 葛 毅, 櫻井 隆雄, ルォン ディン フォン, 阿部 公輝, 坂井 修一: ″インターリーブ型剰余乗算回路の評価″, 電子情報通信学会論文誌, Vol.J88-A, No.12, pp.1497-1505, Dec, 2005.

○ Naoya Hatta, Niko Demus Barli, Chitaka Iwama, Luong Dinh Hung, Daisuke Tashiro, Shuichi Sakai and Hidehiko Tanaka: ″Bus Serialization for Reducing Power Consumption″, 情報処理学会論文誌コンピューティングシステム(ACS 13), Vol.47, No.SIG3, Mar, 2006.

○ 揚妻 匡邦, 河野 健二, 岩崎 英哉, 益田 隆司 : ″需要変化に動的に対応する伸縮自在サーバ群の基本機構″, 電子情報通信学会論文誌, Vol. J88-D1, No. 4, pp. 767-779, 2005.

○ 光来健一・千葉滋: “仮想的な分散監視環境による安全な侵入検知アーキテクチャ”, 情報処理学会論文誌: コンピューティングシステム, vol. 46, No. SIG 16 (ACS 12), pp.108-118、December, 2005

○ 西澤 無我・千葉 滋: “分散ソフトウェアのテストに適したアスペクト指向言語”, 情報処理学会論文誌, 46 巻 7 号, pp.1723-1734, 2005 年 7 月

○ Y. Sugawara, M. Inaba and K. Hiraki : “High-speed and Memory Efficient TCP Stream Scanning using FPGA”, Proc. of 15th Intl. Conf. on Field Programmable Logic and Applications(FPL '05), pp. 45--50, Aug. 2005

○ Hidetsugu Irie, Naoya Hattori, Masanori Takada, Naoya Hatta, Takeshi Toyoshima, Shuichi Sakai: ″Distributed Speculative Memory Forwarding″, IEEE Symp. on Low-Power and High-Speed Chips(COOL Chips VIII), pp.473-482, Apr, 2005.

○ Luong Dinh Hung, Masahiro Goshima and Shuichi Sakai: ″Mitigating Soft Errors in Highly Associative Cache with CAM-based Tag″, IEEE International Conference on Computer Design (ICCD 2005), Vol.2005, pp.342-347, Oct, 2005.

○ Luong Dinh Hung and Shuichi Sakai: ″Dynamic Estimation of Task Level Parallelism with Operating System Support″, International Symposium on Parallel Architectures, Algorithms, and Networks (ISPAN 2005), Vol.2005, pp.358-363, Dec, 2005.

○ A. Sugiki, K. Kono and H. Iwasaki: “A Practical Approach to Automatic

Parameter-Tuning of Web Servers”, Springer, Lecture Notes in Computer Science (LNCS) 3818, Advances in Computing Science - ASIAN 2005, pp.146-159, 2005.

○ H. Yamada and K. Kono: “User-level disk-bandwidth control for resource-borrowing network applications”, Proc. of IEEE/IFIP Network Operations and Management Symposium, To appear.

○ M. Shimamura and K. Kono:” Using Attack Information to Reduce False Positives in Network IDS”, Proc. of IEEE Int’l Symposium on Computers and Communications, To appear.

○ Kenichi Kourai and Shigeru Chiba: “HyperSpector: Virtual Distributed Monitoring Environments for Secure Intrusion Detection”, In Proc. of the 1st ACM/USENIX International Conference on Virtual Execution Environments (VEE’05), pp.197-207, June 2005.

○ Shigeru Chiba and Rei Ishikawa: “Aspect-Oriented Programming beyond Dependency Injection”, ECOOP 2005 -- Object-Oriented Programming, LNCS 3586, Glasgow, pp.121-143, July25-29, 2005

○ Yoshiki Sato and Shigeru Chiba: “Loosely-separated ″Sister″ Namespaces in Java”, ECOOP 2005 -- Object-Oriented Programming, LNCS 3586, ECOOP 2005, Glasgow, pp.49-70, July 25-29, 2005

（２） 特許出願

H17 年度出願件数： 0 件（CREST 研究期間累積件数： 2 件）