「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、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た。それぞれが学会・国際会議などで発表され、若手論文賞などを受賞するとともに、ソフトウェアで２件の特許申請を行った。これからは、要素技術を統合して、超ディペンダブルCPUと超ディペンダブルサーバのシステム技術を開発してゆくこととなる。

2.研究実施内容

平成１６年度は、前年度までで開発したシミュレータをCREST予算で購入したクラスタサーバに実装し、基本アーキテクチャのシミュレーションやソフトウェア研究開発を行った。また、全体の統合イメージを確定させるために、引き続き、１ヶ月から２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１６年度の具体的な実施内容と。統合イメージの現状を記す。

アーキテクチャ研究グループでは、超ディペンダブルチップの基盤となるプロセッサのアーキテクチャとして、従来のチップマルチプロセッサに加えてクラスタ型プロセッサも対象とすることとし、両者のシミュレータとCコンパイラを作成し、これをＰＣクラスタ上で動作させ、さらにいくつかの性能最適化・省電力化技術の提案し、シミュレータに追加・評価して有効性を検証した。チップマルチプロセッサについては、キャッシュ方式、省電力方式を、クラスタ型プロセッサについてはステアリング方式とメモリフォワーディング方式が主な技術である。さらに、ディペンダビリティのための要素技術として、メモリアドレスの動的変更による安全性向上、ソフトエラー検出のための回路構成の研究を行い、評価を行ってその有効性を示した。

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、故障検出から再構成ハードウェアを起動・制御する仕組みについて検討を行った。これは、下に述べるシステムとしてのディペンダビリティ制御技術を確立するための研究と位置づけられ、平成17年度に予定しているプロトタイプモデル構築に備えた。

プロセッサ内で安全性を高めるための暗号回路について、SRT除算を使う方式、モンゴメリ乗算を使う方式の両方でＲＳＡ暗号を効率よく処理する回路を論理設計し、さらにCADを用いてLSI用の実装設計を行った。その結果、高基数のSRT除算を用いる方式、改良型モンゴメリ乗算方式の両者で、少ないハードウェア量で高い効率の暗号回路が実装できることが示された。

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、その構成を提案した（図１）。これまでに提案された各要素技術を統合的に制御するディペンダビリティマネージャ、レガシーコードをディペンダブルコードに変換するコードモーファなどが新しい技術となり、平成１７年度以後に研究が進められる。

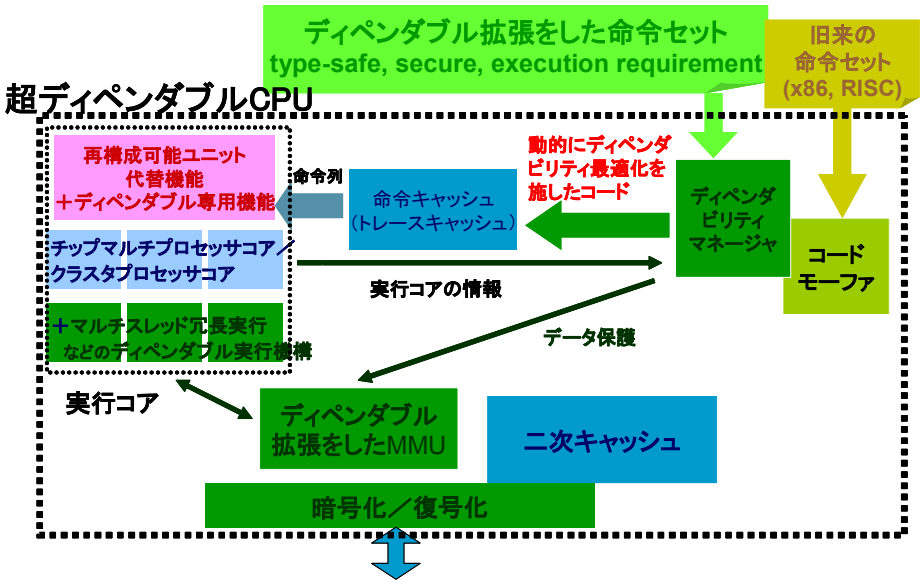

図１．超ディペンダブルCPUチップの構成

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明らかにした。また、インターネットの高速化に対応するため、ＴＣＰマルチストリーム環境でコンテンツマッチングが可能なIDS用のハードウェアアルゴリズムを開発し、これを大規模FPGA上で実装した。IDSハードウェアは、平成１７年度に実働する予定である。

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、研究の最終目標である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の開発に向け、今年度は主に本技術の応用対象である web アプリケーション・サーバの性能改善の技術に取り組んだ。本年度に得られた性能改善のための知見をもとに、今後、そのような知見に基づいた技法を自動的にプログラム中に埋め込む技術を開発してゆく。我々は graceful degradation を web アプリケーション・サーバで可能にするために、そのようなサーバの挙動の典型例を考察し、そのような例の下で過負荷時にも急激な性能低下・システム停止がおこらないようにする制御法を開発した。また、現実に使われているオペレーティングシステムの種類によって、過負荷時の挙動は大きく異なるため、本研究でおこなっているようなミドルウェアによる制御技術を開発し、オペレーティングシステム間の差異を吸収することが大切であることを確認した。

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。今年度は、サーバの管理者によるサーバ・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。昨年度まで開発を進めてきた仮想レイヤの拡張を行い、サーバの挙動を監視しつつ性能パラメータ設定の自動化を行う機構を組み込んだ。今年度は keep-alive 時間という性能パラメータを対象とし、Apache

ウェブサーバを用いた実験によりその有効性を確認した。平成 17 年度には他の性能パラメータについても設定の自動化を図る予定である。また、この研究と並行して、TCP/IP ストリームフィルタと呼ぶネットワーク・フィルタ装置の研究・開発を進めた。TCP/IP ストリームフィルタは、レイヤ7における通信をプロトコル規約に照らし、その正当性を検証する仕組みである。この仕組みにより、未知の不正攻撃に対してもフィルタリングが可能となることが期待される。

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１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．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
４．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。

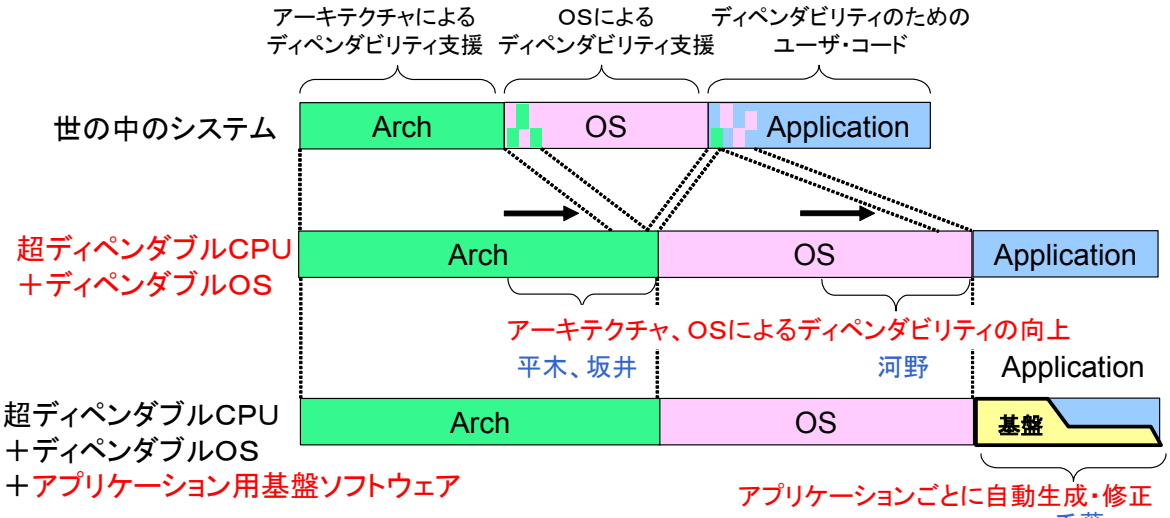

図２．本プロジェクトの統合イメージ

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

3. 研究実施体制

<u>アーキテクチャ研究グループ</u>

東京大学大学院　情報理工学系研究科　電子情報学専攻　　坂井修一

研究実施項目：超ディペンダブルアーキテクチャおよび侵入検知システム

概要：ユーザ向けシステムおよびサーバに求められるディペンダビリティを実現するための基本アーキテクチャとコンパイラを構築する。３年目には、既成FPGAを用いた概念的プロトタイプを構築、評価し、その知見をもとに５年目にプロセッサ・メモリ・ネットワーク系をそろえたディペンダブル基本アーキテクチャとコンパイラ技術を確立する。予算的に可能であれば、プロトタイプＬＳＩの構築を実施する。これによって、ソフトウェアのみでは困難であった、応答性が良く信頼性・安全性・堅牢性の高いシステムが構築され、その技術が検証される。

また、サーバ用の侵入検知システムとして、時系列的に、あるいは対象の分散したイベントの相関分析を取り入れることで実用的なフォールスポジティブと広範囲な侵入検知の両立を目指したものを研究開発する。本システムは、単一のホストでの検知にとどまらずホスト間の協調動作への応用を進める。３年目からは、高速なIDSシステムを提案し、後半にはこれをハードウェア実装する。

ＣＲＥＳＴ後半には、サーバアーキテクチャの開発に侵入検知システムの成果が取り入れられ、また、下記のソフトウェアグループの成果との統合も行われる。

<u>アプリケーション用基盤ソフトウェア研究グループ</u>

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　　千葉滋

研究実施項目：アプリケーション用ディペンダブル基盤ソフトウェア

概要：ディペンダブルなアプリケーション・ソフトウェアを開発するためのプログラミング言語およびソフトウェア開発ツール、そしてミドルウェアの研究をおこなう。まず、アプリケーション・ソフトウェアのプログラムを変換し、信頼性を高めるための機能を自動的に埋め込む技術を、アスペクト指向技術をもとに開発する。これにより、ハードウェアやオペレーティング・システムが必要な機能を提供していてもアプリケーション・ソフトウェアがその機能を使いこなせない、という従来の問題を解決する。また、どのようにして信頼性を高めるか、アプリケーション・ソフトウェア個別の記述を、アプリケーション・ソフトウェアの開発者本人ではなく、ディペンダビリティの専門家がプログラムとして記述できるようにする。このような分担作業により、ディペンダビリティを飛躍的に高めることができる。本技術は、後述のサーバ用ディペンダブル基盤ソフトウェアと統合し、実際の分散処理システム上で実験を行い、実現性・有効性を検証する予定である。また、ディペンダビリティ向上のためのアーキテクチャ技術（前述）を本ツールから利用する統合実験を行い、有用性を検証することをめざす。

<u>サーバ用基盤ソフトウェア研究グループ</u>

電気通信大学　電気通信学部情報工学科　　河野健二

研究実施項目：サーバ用ディペンダブル基盤ソフトウェア

概要：本グループの研究の目標は、広域通信網を利用したディペンダブルな情報サービスを実現する系統的な手法を確立することにある。特に、ディペンダブルな情報サービスを

提供する大規模クラスタ・サーバに焦点を当て、ディペンダブルなサーバを支援する基盤ソフトウェアについて研究開発を行う。具体的には、サーバの実現を支援する基盤ソフトウェアとして、ノード障害の検出、障害からの回復、ノードの追加・削除の自動検出および自動適応、不均一なクラスタにおける負荷分散などを支援する一連の実行時ライブラリ群および実行時システム群の研究開発を行う。サーバの開発者は、これらのライブラリおよび実行時システムを組み合わせて利用することによって、高度なディペンダビリティを有するサーバを実現することができる。数十台から数千台規模で動作するクラスタを対象とし、これらのライブラリ群および実行時システム群は連携して動作して、1）処理能力の拡張性、2）サービスの可用性、3）簡便な保守・管理を達成する。

本技術は、上記のアプリケーション用ディペンダブル基盤ソフトウェアと統合し、実際のユビキタスーサーバ系で実験を行い、実現性・有効性を検証することをめざす。また、ディペンダビリティ向上のためのアーキテクチャ技術（前述）を本ソフトウェアから利用する統合実験を行い、有用性を検証すること、前述の侵入検知システムと本システムの統合をすることなどを検討している。

4.主な研究成果の発表（論文発表および特許出願）

（1）論文発表

○ Cache Coherence Strategies for Speculative Multithreading CMPs:Characterization and Performance Study, Niko Demus Barli, Luong Dinh Hung, Hideyuki Miura, Chitaka Iwama, Daisuke Tashiro, Shuichi Sakai, Hidehiko Tanaka, 情報処理学会論文誌、コンピューティングシス，情報処理学会論文誌　コンピューティングシステム，vol. 45, No. SIG 11 (ACS 7), pp.119-132, Oct. 2004

○ クラスタ型プロセッサのための分散投機メモリフォワーディング，入江 英嗣，服部 直也，高田 正法，坂井 修一，田中 英彦，情報処理学会論文誌コンピューティングシステム(ACS 7)，Vol.45，No.SIG11，pp.94-104，Oct，2004.

○ ファイル移送に基づく分散ファイルシステムの設計と実装，村田 光一，河野 健二，岩崎 英哉，益田 隆司，コンピュータソフトウェア，Vol. 21, No. 4, pp. 43-48, April 2004

○ TCPストリームに対するフィルタリングによるインターネット・サーバの安全性向上，河野 健二(電通大)，品川 高廣(農工大)，ラハト・カビル(電通大)，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. SIG4 (ACS9), pp. 33-44, March 2005

（2）特許出願

H16年度特許出願件数：１件（CREST研究期間累積件数：２件）