

「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术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できる点、(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。

## 2. 研究実施内容

平成15年度は、前年度に引き続き、各要素技術の提案を行い、初期設計・ソフトウェア作成と予備評価、シミュレータ開発などを行った。また、全体の統合イメージを作って方針を決めるために、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15年度の具体的な実施内容を記す。

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シミュレータ基本部とCコンパイラ基本部（坂井研究室で従来から開発されていたコンパイラを本研究用に改良したもの）を作成し、これをPCクラスタ上で動作させた。さらに、基本アーキテクチャであるチップマルチプロセッサのキャッシュ方式、省電力方式、レジスタ間通信方式などについて初期評価を行った。平成16年度には、プロセッサ基本アーキテクチャの中にディペンダビリティのための要素技術を組み込んだ設計を行う。さらには、ディペンダビリティと性能・電力のバランスを検討し、定量的に評価することとなる。

また、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、構成方式を具体的に提案し、シミュレーション評価によってこれを実証した。H14年度は演算回路のみについて再構成可能ロジックで代替機能を提供することを検討したが、H15年度はCPUの主要部全体について同様の提案・評価を行い、検証した。

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検討を行った。SRT除算を使う方式、モンゴメリ乗算を使う方式などでRSA暗号を効率よく処理する回路を検討しており、特にSRT除算について具体的に回路を論理設計した。

侵入検知システム（IDS）については、実際に使用されているネットワーク上でIDSの運用を行い、そこで出力されるアラートの収集を行うとともに、ファイアウォールによるパケットフィルタのログ出力の収集も行った。攻撃行動は単独のパケットによるものではなく、同一の対象に対しての複数の攻撃、あるいは同一の攻撃を複数の対象に行うといった相関性を持つ複数のものによるという特性を利用することでそれら両者の関連付けを行った。パケットフィルタのログという汎用的な機能を利用することでネットワーク上のあらゆる機器からの情報の収集が容易になり、これにより異常検知を行う際に重要な頻度情報を広範囲に集めることが可能となった。

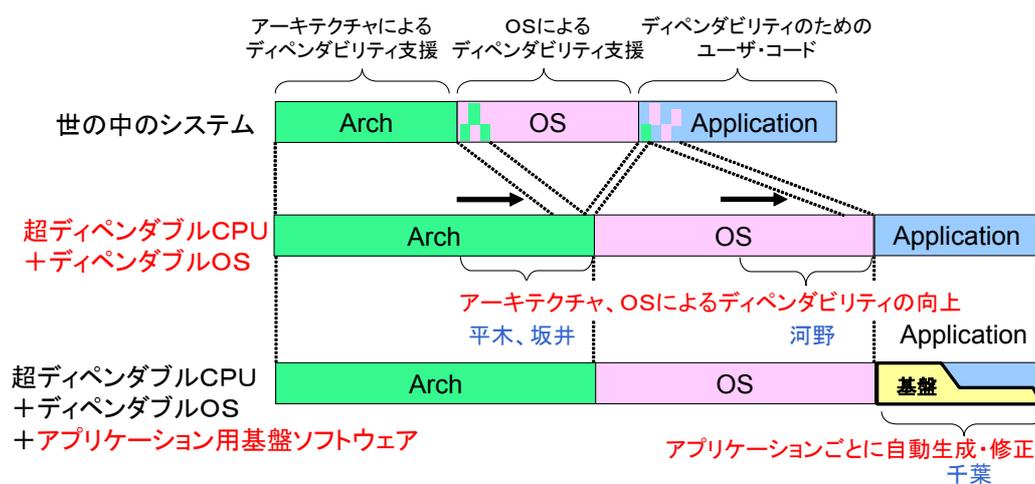
アプリケーション用基盤ソフトウェア研究グループでは、研究の最終目標であるディペンダビリティ機能を自動的にプログラム中に埋め込む技術の開発に向け、我々のグループで過去に開発してきた Javassist の機能拡張をおこない、主に、アスペクト指向技術に基づいたツール開発を具体的な目標に研究をすすめた。Javassist とは、Java 言語をコンパイルして得られる仮想機械語を、プログラム変換するためのライブラリである。H15年度の第一の成果は、Javassist の内蔵 Java コンパイラを開発し、プログラミングインタフェースを大幅に改善したことである。これはソフトウェアを公開すると同時に、国際会議で論文発表をおこなった。次にこれを用いたアスペクト指向開発のためのツール群と

して、Wool と Josh を開発した。Wool は Java プログラムの実行時に、動いているプログラムを止めることなく、一部のプログラムを入れ替えられるようにしたシステムである。これにより、重要性が高く、高いディペンダビリティが求められるソフトウェアを停止せずに、動かしたまま、ソフトウェアの機能拡張や、セキュリティホールの修正などがおこなえるようになった。Josh はアスペクト指向言語 AspectJ に似せた Javassist のフロントエンドである。Javassist は Java 言語のクラスライブラリであるので、利用には Java 言語のプログラムを書かなければならない。これを軽減するために、Java 言語の拡張言語 Josh を開発し、これを使えば Javassist を容易に使えるようにした。

この他に、Javassist のような技術の応用システムの研究を開始し、基本的なアイデアを特許申請した。我々は graceful degradation に対応した web アプリケーション・サーバを開発し、我々の方式によれば混雑時にも急激な性能低下をおこさずに、一定水準のサービスを継続的におこなえることを実験的に検証しようとしている。H15 年度には、予備的な実験により、我々の方式が有望であることを確認することができたので、結果を研究会で発表した。

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・開発を進めた。負荷分散、障害検出、メンバシップ管理等を行う一連のライブラリ群を開発し、それらを統合した高信頼仮想計算機レイヤの実現を行った。さらに、このレイヤ上に高信頼ウェブサーバのプロトタイプ実装を行い、基本設計の有効性の検証を行った。その結果、高信頼仮想計算機の基本設計上の問題点が、今後の検討事項として明確なものとなった。

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1のように行うこととなる。



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1. 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

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年後には、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年後にプロセッサ・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。後半には、高速なIDSシステムをハードウェア実装することを考えている。

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。

#### アプリケーション用基盤ソフトウェア研究グループ

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の研究をおこなう。第一に、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。第二に、完全な自動化が困難な接続については、接続に必要なプログラムを、アプリケーション・ソフトウェア本体から分離されたプログラムとして記述できるようにする。これにより、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接続作業を分担できるようになる。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している。

## サーバ用基盤ソフトウェア研究グループ

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る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（原著論文）発表

- 飯塚 大介、バルリ ニコ・デムス、坂井 修一、田中 英彦、 値予測の軽量効率化方式の提案と評価、情報処理学会ACS論文誌、Vol. 44, No. SIG6 (ACS 1), pp. 65-75, June 2003
- 佐藤 芳樹、千葉 滋、効率的な Java Dynamic AOP システムを実現する Just-in-Time Weaver、情報処理学会論文誌：プログラミング、vol. 44, no. SIG 13 (PR018)、pp. 15-24、October 2003.
- 栗田亮、千葉滋、光来健一、感性を考慮したジョブスケジューリング、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. SIG3(ACS 5), Mar. 2004, pp. 29-37
- 揚妻 匡邦、河野 健二、岩崎 英哉、益田 隆司、モバイルコード技術によるアプリケーション層プロトコルのユーザ透過な配布機構、電子情報通信学会論文誌、J86-D-I(6), pp. 389-401, 2003年6月.
- 河野 健二、金子 済、清水 謙多郎、資源濫用攻撃に耐性のある資源管理方式、情報処理学会論文誌：コンピューティングシステム、Vol.44, No. SIG 11(ACS3), pp. 191-

200, 2003年8月.

- 品川 高廣, 河野 健二, 益田 隆司, 細粒度保護ドメインを用いたsetuidプログラムの特権コード最小化, コンピュータソフトウェア, Vol. 21, No. 2, pp. 25-31, 2004年3月.

(2) 特許出願

H15年度特許出願件数: 2件