研究課題別事後評価結果

1. 研究課題名： ディペンダブル情報処理基盤

2. 研究代表者名及び主たる研究参加者名(研究機関名・職名は研究参加期間終了時点)

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)

主たる共同研究者

河野 健二 (慶応義塾大学理工学部情報工学科 准教授)

千葉 滋 (東京工業大学情報理工学研究科 准教授)

3. 研究内容及び成果

研究課題全体の研究内容及び成果

情報システム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。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した。その主な成果は、(1)アーキテクチャ、サーバ用基盤ソフトウェア、アプリケーション用基盤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を確立した点、(2)情報処理の効率を落とすことなく、また、アプリケーションプログラマに負荷をかけることなく、高度なディペンダビリティを実現した点、(3)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の導入、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た点、(4)CPU アーキテクチャにおいては、ディペンダビリティのためのアーキテクチャ基本要素をディペンダビリティマネージャが呼び出す方式によって、確実にディペンダビリティを向上するようにした点、(4)ソフトウェアにおいては、ディペンダビリティ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した点、(5)ネットワーク侵入防止のために、ハードウェアからソフトウェアまでさまざまなレベルで侵入検知システムを提案・試作し、統合・実証した点、(6)侵入検知システム、WWWサーバなど、全領域にまたがるテーマについては、個々のテーマにおいて国際的水準の成果を出すとともに、統合的・融合的成果をあげることに成功した点、などである。

サブグループ毎の研究内容及び成果

(1) アーキテクチャに関しては、超ディペンダブルプロセッサという形で、近未来に必要なさまざまな高信頼化・安全化技術を研究開発するとともに、ディペンダビリティマネージャを用いてこれを統合的に管理する方式を提案・評価・検証した。ここで、要素技術として開発したものは、耐タンパ技術(アドレスランダムマイズ技術、耐ソフトウェアタンパ・モード)、プログラム監視技術(インジェクションアタック検出の高精度化、由来に基づいた情報漏洩保護技術、値範囲伝搬を利用したプログラム静的解析技術)、耐エラー技術(組合せ回路における Single Event Transient の検出、縦横パリティによるキャッシュアーキテクチャ、ばらつきを考慮したスペアビットの利用法、レジスタ書き込み時のタイミングエラー検出、エラー回復アーキテクチャ)、ディペンダビリティ管理技術(メモリ上データのタグ管理方式、柔軟なタグ伝搬アーキテクチャ)、耐永久故障アーキテクチャ(再構成による耐永久故障アーキテクチャの提案と検証)である。

高速侵入検知システムの研究では、10ギガビット/秒を越える速度でのTCPストリーム内容検査をバックボーンネットワークで集中的に行える方式を提案し、これを実装して有効性を検証した。高度な侵入検知のために、TCPストリームフィルタと呼ばれるソフトウェアを開発し、亜種のアタックなどより狡猾な侵入をも検知できることが示された。

(2) サーバ用基盤ソフトウェアでは、ウェブサーバのディペンダビリティ向上のための諸技術の研究・開発を行った。具体的には、ウェブサーバの性能パラメータの自動調整機構およびウェブサーバの分散ホスティングのための基盤を確立することができた。

(3) 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、アスペクト指向に代表される最新のソフトウェア技術をディペンダブルシステムの構築に応用する研究をおこなった。本研究グループの研究は、ディペンダビリティのための機能を利用するコード(ディペンダブル・コード)を数個のモジュールに集約し、開発者の中の少数のディペンダビリティの専門家によって開発保守ができるようにした。

(4) 統合研究として、侵入検知システムと超ディペンダブルWWWサーバをグループ間協力のもとに研究開発し、評価・検証を行った。

成果は、主要なジャーナル論文誌・国際会議などの場で発表され、いずれも高い評価を得た。また、特許取得(国際特許を含む)、フリーソフトウェアなどの公開によって、広く有用性が確認されることとなっている。

さらに、CREST シンポジウムなどの機会には、(1) 超ディペンダブルプロセッサ(FPGA ボードによる超ディペンダブルプロセッサを試作。タンパ耐性、アタック耐性、故障耐性のそれぞれについての具体的な実験・デモ)、(2) 高速侵入検知システム(2つの10ギガビット・イーサネットインタフェースを持つ侵入検知システムの展示・実演)、(3) TCPストリームフィルタ(TCPストリームフィルタの入ったPCの展示、ウェブサーバに対して攻撃を仕掛け、その攻撃メッセージを検出したり遮断したりする様子を見せた)、(4) サーバ用基盤ソフトウェア(ウェブサーバの性能パラメータ自動調整機構についての実演)、(5) アプリケーション用基盤ソフトウェア(開発したアスペクト指向プログラミング言語 GluonJ を用いて実装した河川水量モニタシステムおよび TV 番組紹介 SNS の展示発表)などの展示・デモを行った。

4. 事後評価結果

4-1. 外部発表(論文、口頭発表等)、特許、研究を通じての新たな知見の取得等の研究成果の状況

1) 外部発表、特許出願等

この研究分野は論文投稿が比較的難しい領域であるが、ジャーナル26件、査読付き国際会議34件、他発表135件で大変活発な発表が行われた。国際会議のキーノート講演や招待講演も多く、成果が広く世界に伝わることとなった。

特許は国内出願4件、外国出願1件である。もう少し分野を広げて、数を増やすことも可能であったと思われる。しかし、アーキテクチャや回路レベルの特許があり、大きな影響力を持ちえる基本的な特許が出されており、その努力は評価される。

2) 研究成果の状況

研究成果は、大変多く出ている。アーキテクチャについては、今後のデバイス微細化に伴い出てくる回路の不安定性をアーキテクチャレベルで高信頼化するための様々なハードウェアやソフトウェアなどの基本のアイデアがあり、要素技術として今後期待できる。また、外から入ってきた危険な情報やプログラムを、情報にその出自を表すタグを付けることで検出する基本アイデアが発明され、侵入検知システムでは、従来のシグネチャ方式に代えて正しいパケットの定義を入れるという新しい概念の方式が案出され有効性が示された。今後実用面から評価がすすめば広く使われる可能性がある。また、サーバ用基盤ソフトウェア関係では、負荷変動に対する脆弱性や設定ミスに対する自動修復などの面白い手法が生み出され、応用レベルでは、アスペクト指向の考えかたAOPを応用の安定化に採用し、応用とは別に記述されたプログラムにより、応用の性能チューニングをおこなうことを可能にした。これにより、AOPの有用性を、実用的なソフトウェアの開発を通して実際に検証し、この分野の国際会議で高い評価を得、新たな手法の可能性を開いた。

3) 当初の研究計画に対する、成果の妥当性

今後の情報システムに特に求められる、情報システムのディペンダビリティを抜本的に向上させることを真正面

から取組み、その基幹技術をアーキテクチャ、基盤ソフトウェア、プログラミングに渡って開発した。これらを元に、今後の様々な取組が可能となる。また、要素技術に留まらず、デペンダビリティの革新的・包括的な技術を実現した。根幹となるデペンダブルシステム設計の設計論を確立するまでには到らなかったものの、当該問題は根源的に極めて難しい問題であり、成果としては妥当であって、よくそれを達成したといえる。

4 - 2 . 成果の戦略目標・科学技術への貢献

1) 得られた研究成果の科学的・技術的インパクト

デペンダブル技術は歴史は長いものの、統一的な取り扱いが極めて難しい領域である。従来、情報システムのデペンダビリティへの対応技術はアドホックな対応しか存在しなかったが、アーキテクチャから応用レベルに至る基本的な対応技術のセットを提案し、それぞれの効果を定量的に評価した。これによって、従来のコンピュータシステム研究とは質の異なった新技术を複数提案できており、情報システムの構築にインパクトを与えた。更に、学術的にも情報の信頼性評価手法を開発するとともに、新しいプログラミング手法として、アスペクト指向技術の有用性を実用的なソフトウェアの開発を通して実際に検証し、この分野の国際会議で高い評価を得た。これらにより新分野を開いたといえる。

2) 国内外の類似研究成果と比較した、研究成果のレベルと重要度

国内的にみると、この分野では疑いも無くトップレベルにある。国際的にみると、デペンダビリティ技術の草分けとして、本研究は世界を先導した。要素技術的にみると、高信頼なアーキテクチャ技術は、世界的に様々なものが出されつつあり、本研究がすべてそれらを包含する訳ではないが、その幾つかでトップであって、総合的にみれば米国の先端と同レベルにある。侵入検知システムに関しては、効率よいハードウェアアルゴリズムの提案で、40Gbps という超高速なシステムの実現性を示し、世界最高性能を示した。アスペクト指向プログラミング技術に関しては、その有効性を始めて具体的に示し、国際的に認知されており、世界トップレベルである。

3) 研究成果のさらなる展開

デペンダブルアーキテクチャについては、この手法をベースに、今後出てくる微細実装技術、35ns 以下のテクノロジーで、プロセッサなどの論理回路を実現する場合に発生することが予想されている回路の不安定性に対処する技術として使われ実用化されることが考えられる。この分野は、難しい領域ではあるものの地道な研究を推進する必要がある領域でもあり、今後に期待したい。とりわけアーキテクチャなどは世界的な動きを取り込み、ここで生まれた考えかたを世界の主流にしてゆく戦略も必要であろう。

侵入検知システムについては、高速システムをハードウェアで実現する場合に有効である。フィルタ技術についても、従来対応が困難であった新たな脅威に対応する技術として実用される可能性がある他、応用レベルのプロトコル情報を用いた高精度な侵入検知手法として発展することも考えられる。プログラミングの分野では、開発したアスペクト指向言語 GluonJ を更に普及させ、様々な応用を開拓し、求められる信頼性や安全性、安定性などへの要請に、応用本体とは独立な形で対応する一般的な手法として発展することが期待できる。

このように、要素技術が多方面に渡っており、展開すべき多くの研究が今後とも存在する。産業界への応用も十分期待できる。

4 - 3 . その他の特記事項(受賞歴など)

1) 研究体制等

アーキテクチャ、OS、アプリケーションソフトウェアの各領域の研究者が協力して、デペンダビリティという一つの目的に向かって仕事をするという、最近では稀な構成のグループである。これによってこの分野の技術イメージが明らかになり、世界的にも認知されることとなった。

この成果は、STARC や新しい CREST に引き継がれており、本研究の成果は産業界にも学会にも認められていることを示している。この分野は今後とも情報社会の根幹となる安全性を確保するために必須となる技術開発分

野であり、国をあげて技術開発に積極的に取り組んでいく必要がある。

2)総合的評価

今後の情報社会にもとめられるデペンダビリティをサポートする総合的な研究として、理論的にも実験的にも確実な実証データを提供し、大きな成果を挙げた。このデペンダブル基盤というむずかしい課題に取り組み成果を得たことは高く評価される。これらをベースに今後、多くの研究や実用化がなされるであろう。そういう意味でCRESTとしても十分評価できる研究である。