氏　　名　織茂昌之（おりもまさゆき）

学位(専攻分野)　博　士（工　学）
学位記番号　論工博第3529号
学位授与の日付　平成12年7月24日
学位授与の要件　学位規則第4条第2項該当
学位論文題目　計算機システム高信頼化技術に関する研究

論文調査委員　(主査)教授 井上紘一　教授 土屋和雄　助教授 幸田武久

論文内容の要旨

本論文は，近年主流となっている分散計算機システム構成を主な対象として，セキュリティを含む広い意味での信頼性向上のための技術開発を目的とし，現実のアプリケーションからのニーズに沿って行われた研究の成果をまとめたもので，5章からなっている。

第1章は序論であり，研究の動機と目的，関連研究の状況と問題点，研究の具体的対象，本論文の全体構成について述べている。

第2章では，分散システムを構成する各サブシステムに自律性を持たせることにより，システムとしての耐故障性，オンライン拡張性，オンライン保守性を向上させることを目的として提案されたシステムアーキテクチャである自律分散システム構成について述べ，その具備すべき基本機能について考察を加えている。ついで，この自律分散システム構成を前提として，システム信頼性向上を支援する以下の2方式，即ち(1)リアルタイム処理が要求される制御システムを対象として，アプリケーションプログラムのリアルタイム環境でのテストを実現するためのオンラインテスト方式，および(2)処理結果データの保証が要求される情報システムを対象として，重要なデータをネットワーク接続された任意の計算機のディスクに多重配置するためのファイル多重化方式，を提案している。(1)のオンラインテスト方式を実装した自律分散システムとして，プラント制御システムに適用された例をあげている。(2)のファイル多重化方式の適用例として，国際的な仲介業務を行っている中規模会社における伝票発行業務システム及び中規模生産ラインにおける生産管理システムについて述べている。これらの適用例により，提案された2方式の有効性を検証している。また，広域通信ネットワークを対象として，そこで提供されるサービスの実行状況を柔軟に監視するゲートウエイシステムへの自律分散システムの適用についても考察している。

第3章では，システムを構成する各サブシステム間の連携により，システムとしての機能が達成されるという前提に基づき，システム分割のモデル化およびシステム分割の定性的評価を行い，システム分割に対する設計基準を導出する手法を与えている。すなわち，部分的障害発生後のサブシステム間結合の再構成という観点からシステムをモデル化し，部分的障害発生後の機能の達成度合いを評価する機能信頼性評価尺度を用いて，システム分割を評価する方法を与えている。さらに，自律分散ループネットワークシステムを対象として，上記手法を適用して単一ループ構成とマルチループ構成のトレードオフについての評価を行い，ノード数が大，すなわちシステムの規模が大きくなると，マルチループ構成に分割した方がより高い耐故障性を達成できることを具体的に示している。

第4章では，計算機システムにより実行される情報処理アプリケーションのセキュリティを保証するために，評価対象のモデル化，脅威の抽出，対策方針の導出，セキュリティ目標の確立，およびセキュリティ対策の策定，の5段階プロセスから構成される対策立案手法を提案している。ケーススタディとして，ICカードを利用したチケット販売・入場ゲート管理システムのセキュリティ対策立案に適用した例を述べ，体系的な脅威の抽出とそれに対する対策の立案が効率的に行えることを確認し，この手法の有用性を明らかにしている。

第5章では，本論文で得られた成果を要約するとともに，ネットワークを中心とした情報システムに対するセキュリティ

まで含めた広い意味での信頼性への要求は，今後ますます高まってゆくであろうことを述べ，結論としている。

論文審査の結果の要旨

本論文は，自律分散計算機システム構成を主な対象として，セキュリティを含む広い意味での信頼性向上のための技術開発を目的とし，現実のアプリケーションからのニーズに沿って行われた開発研究の成果をまとめたもので，得られた主な成果は以下の通りである。

1．リアルタイム処理が要求される制御システムを対象として，アプリケーションプログラムのリアルタイム環境でのテストを実現するためのオンラインテスト方式を提案した。さらに，実際のプラント制御システムに適用しその有効性を検証した。

2．処理結果データの保証が要求される情報システムを対象として，重要なデータをネットワーク接続された任意の計算機のディスクに多重配置するためのファイル多重化方式を提案した。さらに，実際の伝票発行業務システムおよび生産管理システムに適用しその有効性を検証した。

3．広域通信ネットワークを対象として，そこで提供されるサービスの実行状況を監視するゲートウエイシステムへの自律分散システムの適用について考察し，システムのモデルを提案した。さらに，このモデルを実現するための機能要件を明確にした。

4．システム分割のモデル化およびシステム分割の定性的評価を行い，システム分割に対する設計基準を導出した。さらに，自律分散ループネットワークシステムに適用して単一ループ構成とマルチループ構成のトレードオフについての評価を行い，システムの規模が大きくなると，マルチループ構成がより高い耐故障性を達成できることを具体的に示した。

5．計算機システムにより実行される情報処理アプリケーションのセキュリティを保証するために，評価対象のモデル化，脅威の抽出，対策方針の導出，セキュリティ目標の確立，およびセキュリティ対策の策定，の5段階プロセスから構成される対策立案手法を提案した。さらに，ICカードを利用したチケット販売・入場ゲート管理システムのセキュリティ対策立案に適用し，この手法の有用性を明らかにした。

以上要するに本論文は，計算機システム上のプログラム，データ，サービスの信頼性を向上させるために，分散計算機システムが具備すべき機構，信頼性の観点からシステム構造を決定するための評価手法，情報セキュリティを守るための対策立案手法を提案したもので，その成果は学術上，実際上寄与するところが少なくない。よって，本論文は博士（工学）の学位論文として価値あるものと認める。また平成12年5月22日，論文内容とそれに関連した事項について試問を行った結果，合格と認めた。