「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」
平成 18 年度採択研究代表者

石川　裕

（東京大学情報基盤センター　教授）

# 「並列・分散型組込みシステムのための ディペンダブルシングルシステムイメージ OS」

## 1. 研究実施の概要

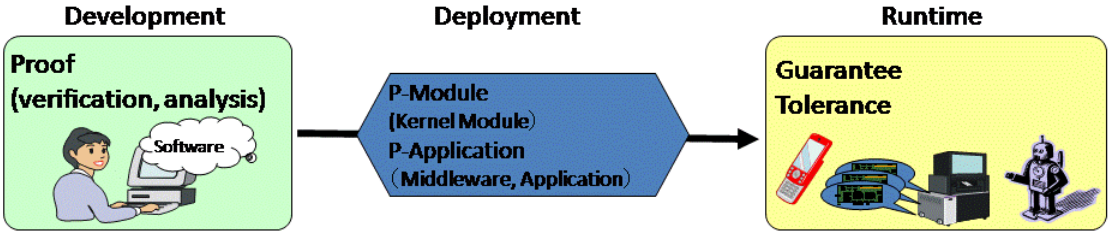
本研究ではネットワークで接続された組込みコンピュータによるデータベースサーバや高性能計算システムを実現するための高信頼高性能組み込み並列分散オペレーティングシステムを研究開発する。処理能力に応じて、ディスクを搭載したコンピュータ群、マルチコア CPU とメモリだけを搭載したコンピュータ群が適時ネットワークでつながれるクラスタシステムを想定し、Linux を基に、高信頼単一システムイメージを提供する並列分散 OS を実現する。これにより、オペレーティングシステムレベルでハードウェアの耐故障機能および実時間性を実現する。

## 2. 研究実施内容

本年度は、プロジェクト開始の初年度であることから、佐藤チーム、徳田チーム、中島チーム、前田チームと共に全体コンセプトおよびシステムアーキテクチャ、デモイメージ案について議論した。デモイメージについては、平成19年度も引き続き検討事項となっているため、本報告書では、全体コンセプト並びにシステムアーキテクチャについて報告する。

### 2.1 全体コンセプト

コンピュータシステムがディペンダブルであるために、ソフトウェアの開発・配置・保守というライフサイクルに対して、我々は次のようなコンセプトを提案した。




- ソフトウェア開発時にソフトウェアの論理的機能、時間制約、脅威の可能性を検証あるいは解析する。

- 保証すべき性質を Failure-proof、Energy-waste-proof、Performance-degradation-proof、Threat-proof の4つに分類した。これらを総称して*-proof と呼んでいる。これらについては後述する。
- ソフトウェア開発時に検証あるいは解析したプログラムは、P-module（あるいは P-application）として提供される。
- 静的に検証・解析できない性質（予測不能性）は、実行時耐故障性機構により対処すると共にロギングする。

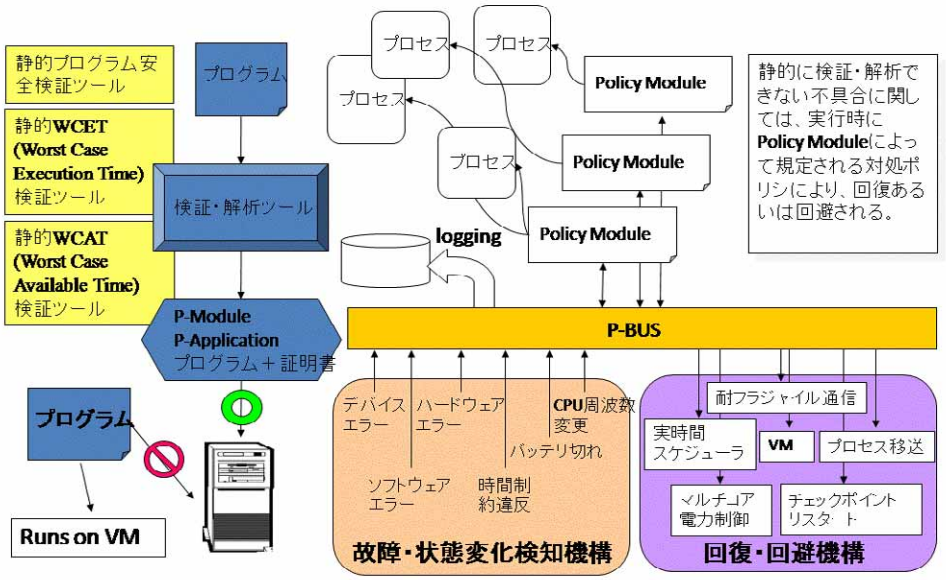
ソフトウェア開発時、実行時に保証する4つの性質についてその概要を示す。

- Failure-proof
  - **ソフトウェア開発時：ソフトウェアの安全性、耐故障性検証**
  - **実行時：故障を検知／予測し、故障回復、故障隔離保証**
- Energy-waste-proof
  - **ソフトウェア開発時：消費電力量解析、省電力復帰時間解析**
  - **実行時：持続システム保証**
- Performance-degradation-proof
  - **ソフトウェア開発時：実時間性および性能解析**
  - **実行時：実時間性および性能保証**
- Threat-proof
  - **ソフトウェア開発時：アタック回避検証**
  - **実行時：アタック回避保証**

アプリケーション分野によってこれら性質の実現方法は異なる。そこで、アプリケーション分野を携帯電話分野、OA・情報家電・センサー分野、サービスロボット・FA 分野に分け、各チームがどの分野においてどのような性質に対するディペンダビリティを実現するかを整理した。以下に示す。

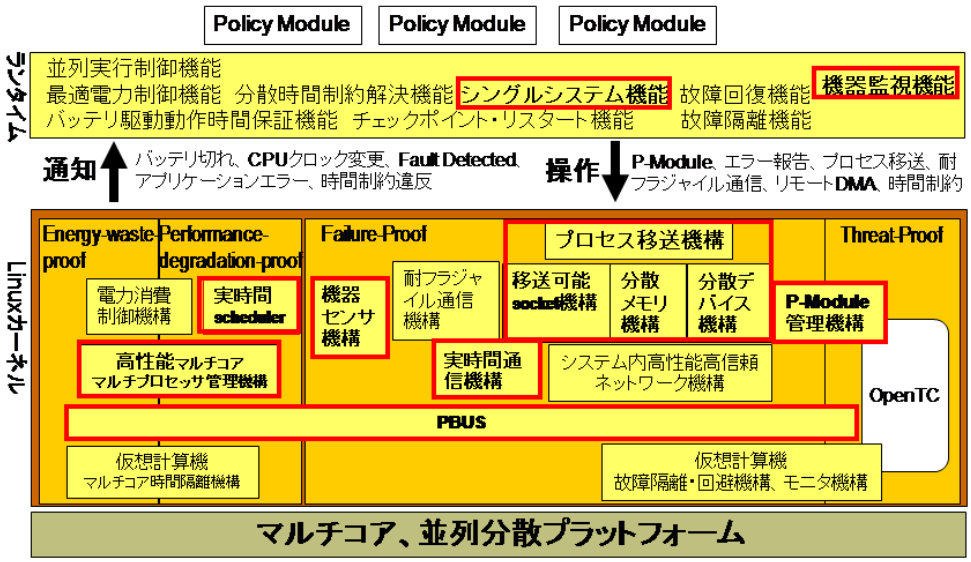
2.2 システムアーキテクチャ

本領域で開発されるシステムの全体の概念レベルシステムアーキテクチャを以下の図に示す。以下の図で左側は開発時のツールを示している。静的プログラム安全検証ツールは前田チームが開発する。静的 WCET 検証ツールは石川研究室が CREST「ヒューマノイドのための実時間分散情報処理」(分担研究者、2008 年 9 月終了)において開発中のツールを発展させて実現する。静的 WCAT 検証ツールは徳田チームが開発する。




上図右側は*-proof を支援するためのオペレーティングシステム機構の概念図である。*-proof を実現するために、ハードウェアやソフトウェアの状態を検知する機構、検知したハードウェアあるいはソフトウェアの不具合を回復・回避する機構の大きく2つの機構を導入する。回復・回避機構は基本的な機構を提供するものであり、ポリシモジュールによって故障時の対応が決められる。P-BUS は、検知機構、回復・回避機構、ポリシモジュール、OS カーネルとの間のインターフェイスおよびシステム全体の整合性をとるためのソフトウェアモジュールである。

下図は、Linux カーネルにおけるシステムアーキテクチャである。図中、石川チームが開発を担当する部分を赤枠で示す。これらモジュールのプロトタイプを平成19年度開発する。




## 3. 研究実施体制

(1)「石川」グループ

①研究分担グループ長:石川　裕(東京大学　教授)

②研究項目

・高信頼組込シングルシステムイメージ OS