

ロバストな組み込み向けオペレーティングシステム)

開発者： 追川 修一, 菅谷 みどり, 岩崎 匡寿
鈴木 裕介, 松浦 杏子, 小林 宣幸

- 開発の目的
 - 資源管理と仮想化を組み合わせ、将来の組み込みシステムのプラットフォームとなる環境を提供する
- 機能と特徴
 - 多様化した資源要求への対応  資源管理, 資源保証
 - セキュアな環境の提供  OS環境の仮想化
 - 障害回復する仕組みの提供  障害回復機能

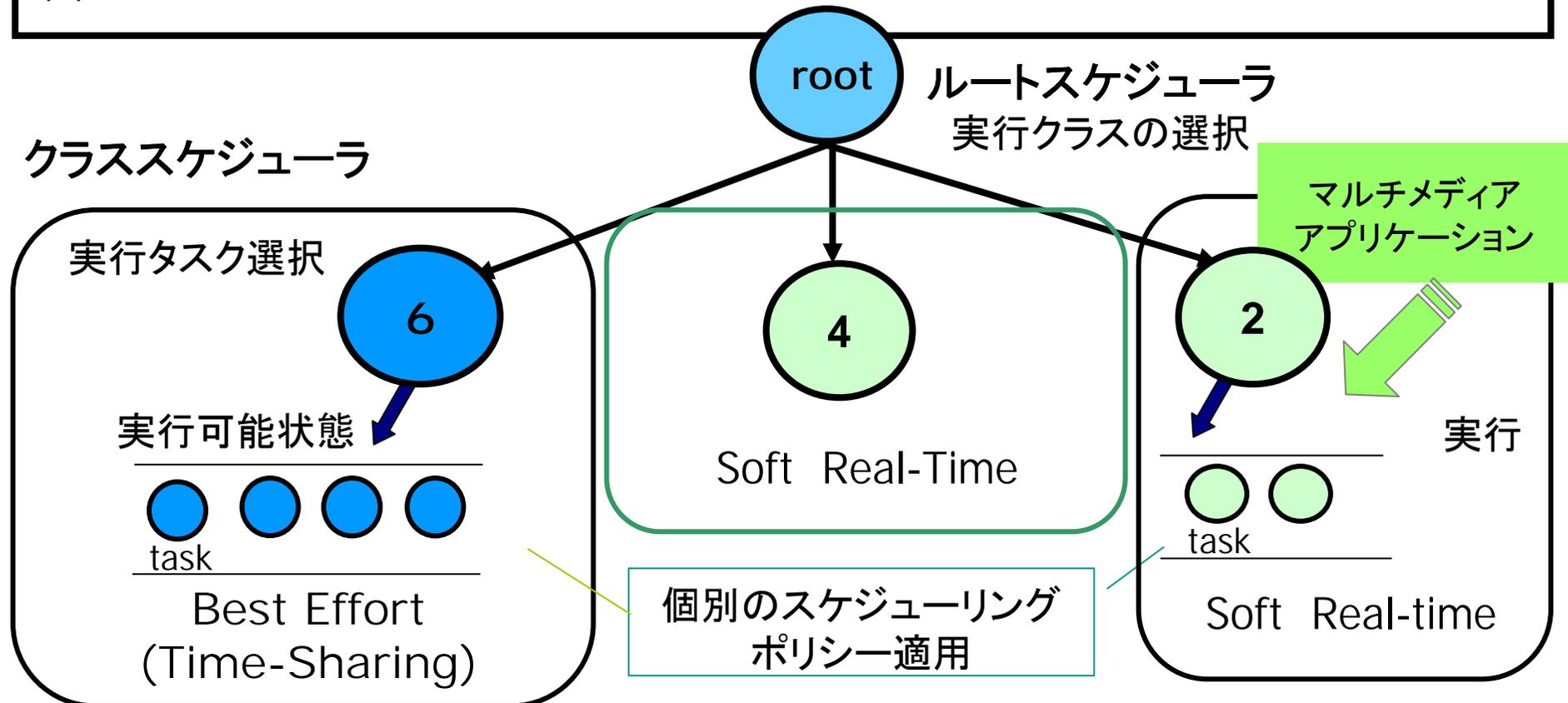
システムが安定して動作する環境 = ロバストな環境

 ロバストな環境を提供する OS の開発

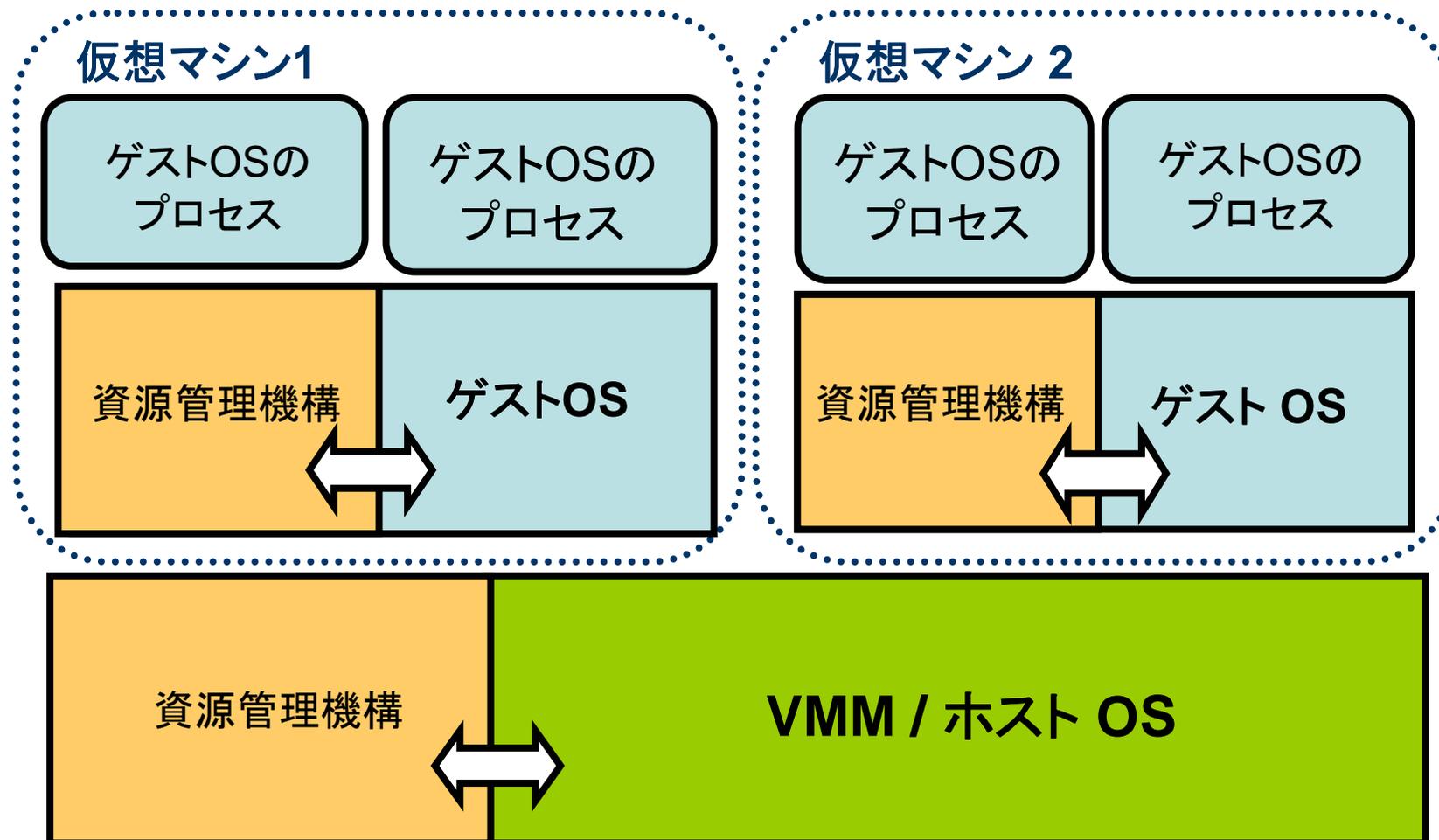
資源管理機能

フェアシェアベースのクラス別スケジューラ

- (1) 保証型 + 複数ポリシーのサポート ⇒ **ウェイト**に応じた公平な割り当て (Fair Share)
- (2) アプリケーションドメインの分離 ⇒ **パーティショニング**によるセキュリティの確保
- (3) クラスの追加/削除が可能 ⇒ **柔軟なシステム**設計



階層的資源予約機構



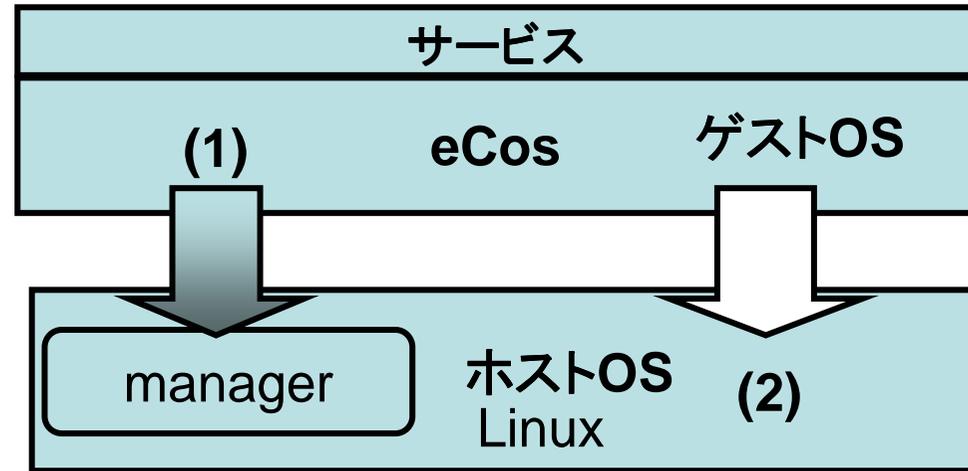
- ・VTSC (Virtual Time Stamp Counter) 実装により正確に動作を測定
- ・Linux (ホストOS) + UML (User Mode Linux) (ゲストOS)

障害回復機能

障害発生前

(1) 定期的にハートビートを送信

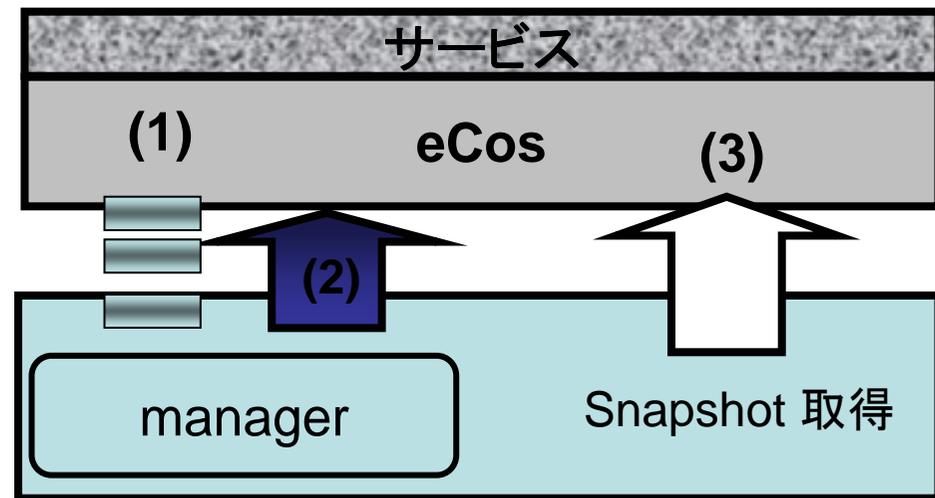
(2) 定期的にデータを送信
(Snapshot 保存)



(1) ハートビートの停止を
ホストOS が検出

(2) ホストOSの監視プロセスが
eCos を再起動
→ eCos とサービスが起動

(3) サービスがスナップショット
取得 (元の状態を回復)



障害発生後