トップエスイー修了制作

高可用クラスタソフトウェアの設計モデル検証

富士通株式会社　小島隆弘　kojima.takahiro@jp.fujitsu.com

開発における問題点

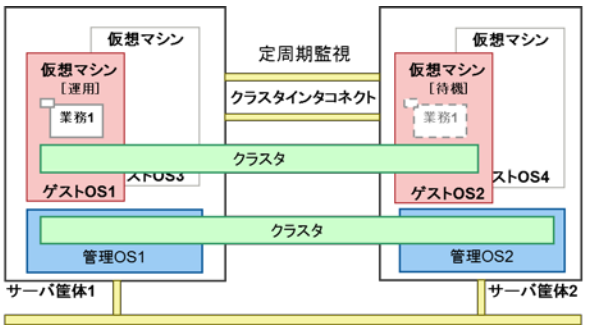
サーバ仮想化環境への適用などで故障要因と要因間の依存関係が複雑化し、どのようなパラメタを与えた場合に高可用クラスタソフトウェアの基本的特性が満たされるかを机上のシーケンス検証により完全に保証することは困難

手法・ツールの適用による解決

Promela言語で高可用クラスタソフトウェアの動的な振舞いを記述、LTL論理式で高可用クラスタソフトウェアの基本的特性を記述し、これらをモデル検査器SPINに入力することにより、網羅的に故障発生時の実行シーケンスを評価

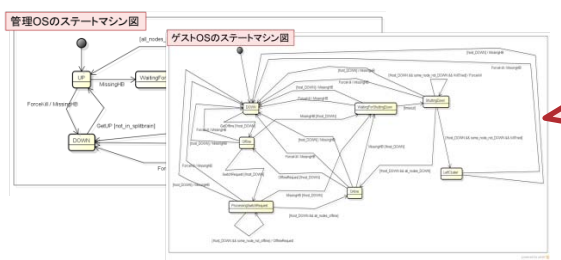
SPINによるハイブリッドクラスタの記述

2ゲストOSノード、2管理OSノードからなるハイブリッドクラスタ



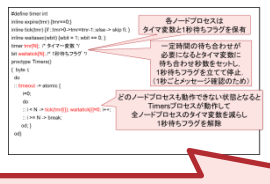
Promela言語による各ノードの動作記述

強制停止によるノードダウン



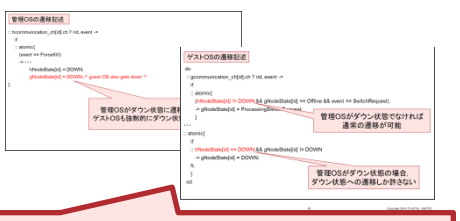
優先的メッセージ処理により特殊な強制停止割込みを表現

生存優先度に応じた強制停止の待ち合わせ



カウントダウンタイマにより状態爆発を防止
1秒待ちフラグにより待ち合わせ中の強制停止に対応

ノード間の依存関係



他ノード状態の強制書換えにより意図しないデッドロックを排除

高可用クラスタソフトウェアの基本的特性

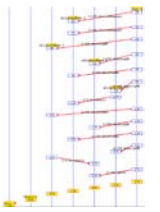
- 複数ノードが同時にオンラインにならない
- 故障発生後に業務継続可能なノードがオンラインになる

LTL論理式による性質記述

[]!((ゲストOS1状態 == Online) && (ゲストOS2状態 == Online))
[]<>((ゲストOS1状態 == Online) || (ゲストOS2状態 == Online))

検証結果

設定	反例	意味
通常	なし	現状の設計は妥当
生存優先度制約違反	**あり**	制約は妥当
スプリットブレイン解決時間制約違反	**あり**	制約は妥当



SPINによるモデル検査は
高可用クラスタソフトウェアの設計検証に有効