トップエスイー修了制作

ストレージシステム機能仕様策定における Event-B適用検討

(株)日立製作所　松下 貴記　takaki.matsushita.xa@hitachi.com

開発における問題点

多機能化したストレージシステムに対し，更なる新機能の開発が要求されている．新機能の上流仕様検討者は，以下の問題を抱えている．

1. 既存機能仕様と新機能仕様が矛盾しないことの検証が困難
2. 既存機能の仕様把握が困難

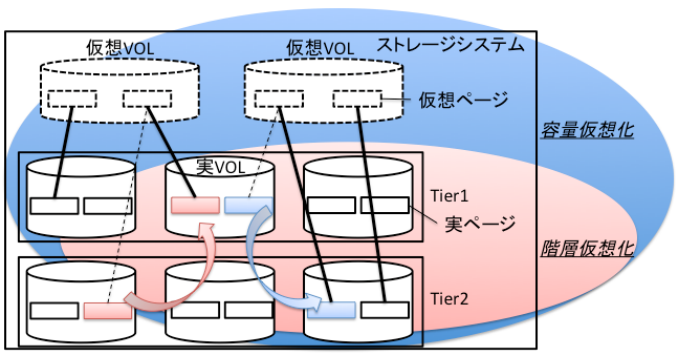
手法・ツールの適用による解決

既存機能仕様をEvent-B抽象モデルに集約し，抽象モデルをリファインメントし，新機能仕様を詳細モデルとして記述・証明を行うことで，多機能化したストレージシステムの新機能開発における問題の解決に有効であった．一方，Event-Bによる仕様記述には暗黙知が潜んでおり，記述方法の形式知化の必要性を認識した．

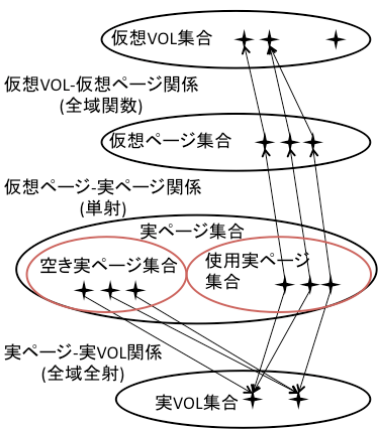
ストレージシステム機能におけるEvent-B適用実験

- ストレージシステムの容量仮想化機能を抽象モデル，階層仮想化機能を詳細モデルとし，Event-Bで厳密な仕様記述及び証明責務の証明を実施．上流仕様検討工程におけるEvent-Bによる仕様記述の有効性を確認．

【ストレージ容量仮想化・階層仮想化】



【モデル化方針】

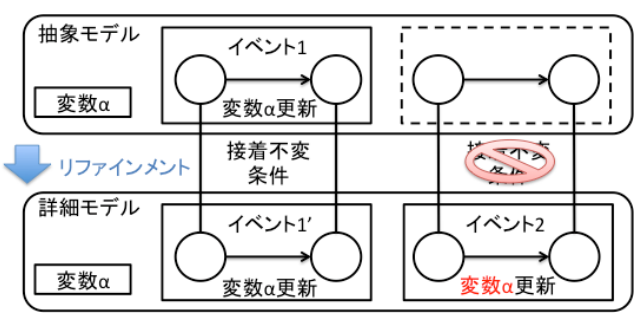


#	Event-B記述の有効性
1	仕様検討者・レビュアーの不安の解消
2	上流工程から厳密な仕様を記述可能
3	既存仕様と矛盾しない仕様を策定可能
4	新機能で保証すべき既存機能の仕様を把握可能
5	既存仕様の認識違いのリスクを低減

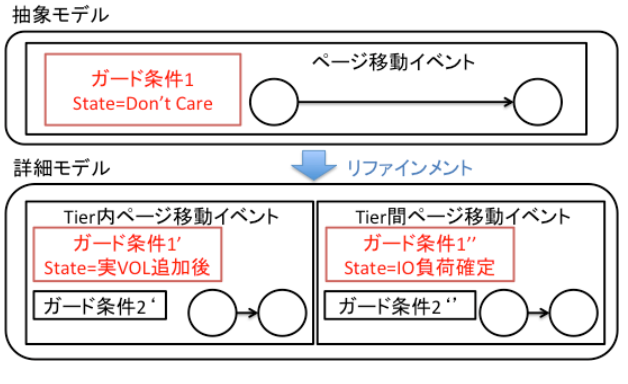
Event-B記述暗黙知の形式知化

- 証明・リファインメントをスムーズに実施する為，記述ノウハウ(暗黙知)の整理を実施．
- 得られた暗黙知：抽象モデルで証明済みの仕様に矛盾する仕様を詳細モデルで記述してはならない
  →詳細モデルの記述内容を予め見通す事は非常に難しい．リファインメント計画表を作成し，見通しに役立てる．

【暗黙知1】:
変数更新可能性の考慮
詳細モデルの新規追加イベントで抽象モデルの変数を更新不可



【暗黙知2】:
イベントガード条件一般性の考慮：
抽象モデルのガード条件は詳細モデルのガード条件を包含すべき



【リファインメント計画表】
暗黙知1・2の判断の容易化