DEOS-FY2009-PP-01

21世紀の組込みシステムとディペンダビリティ

Challenge to Open Systems Dependability

2009年9月4日

所　眞理雄

JST/CREST 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 プロジェクト総括

（株）ソニーコンピュータサイエンス研究所

プロジェクトの背景

- 組込みシステムの高度化、複雑化に対応できるシステム構築技術の要求
  - 組込みソフトウェアの巨大化によりソフトウェア部品のブラックボックス化などシステムの隅々までの理解が不可能
  - 組込みシステムのネットワーク化による情報漏洩、ウィルス、不正アクセスシステムダウンなどの利用者の安全・安心を脅かす諸問題
- システム運用中の要求や環境の変化に安全に対応できる技術の要求
  - 要求変更による仕様の変更
  - ネットワークやネットワーク上のサービスの変更
- 開発から運用終了までのライフサイクルに亘るディペンダビリティ確保の重要性
- 組込みシステムにおけるサービスや製品の提供者の責任の増大

新しい視点が必要？

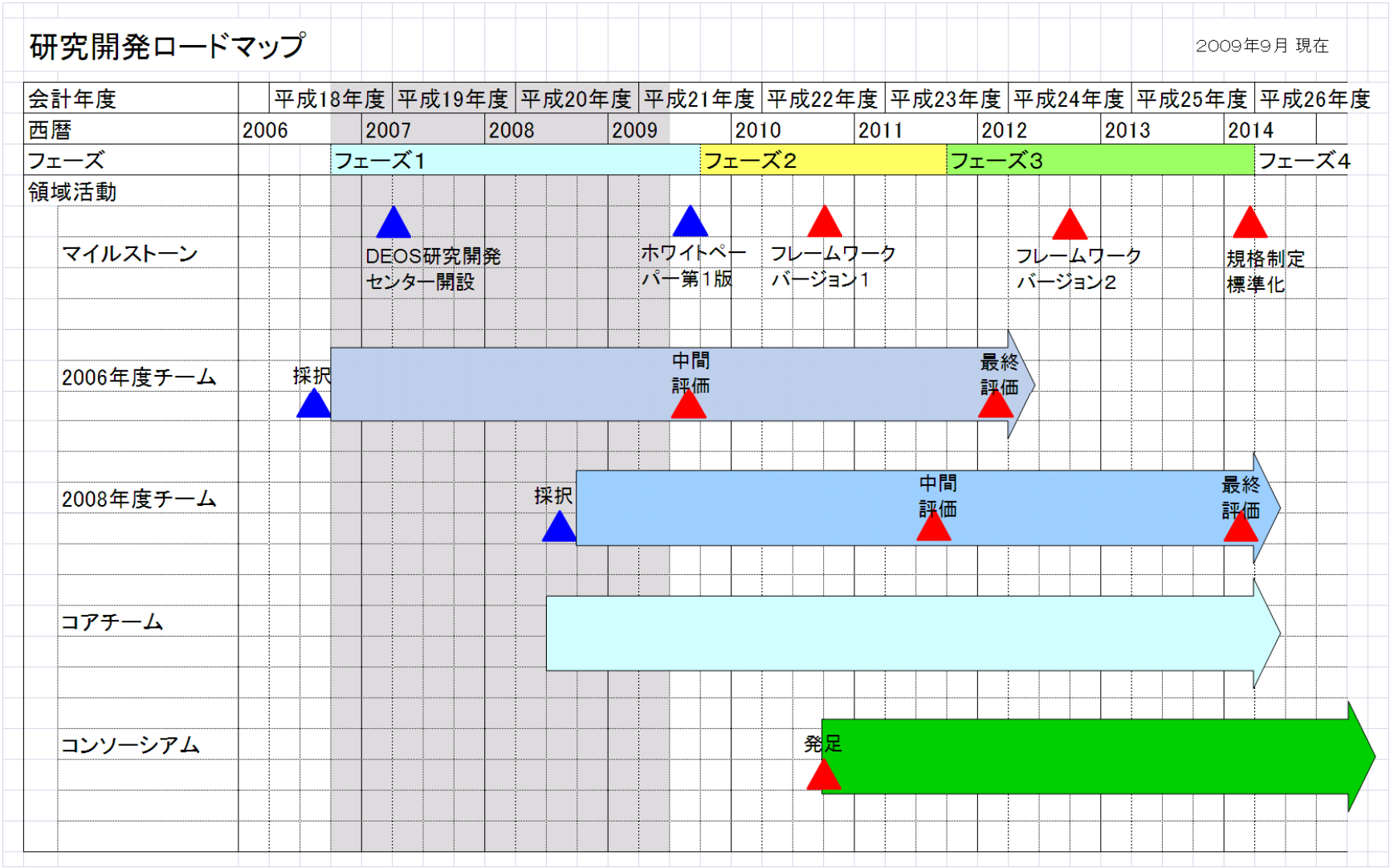
- これらの要求はオープンシステムへの対応を意味する
  - これまでのディペンダビリティはクローズドシステム仮説のもとでのもの
- オープンシステムに対応した新しいディペンダビリティの考え方が必要
  - これに基づき、開発時から運用終了までのライフサイクルに対応したディペンダブルソフトウェアを構築

本プロジェクトの目的

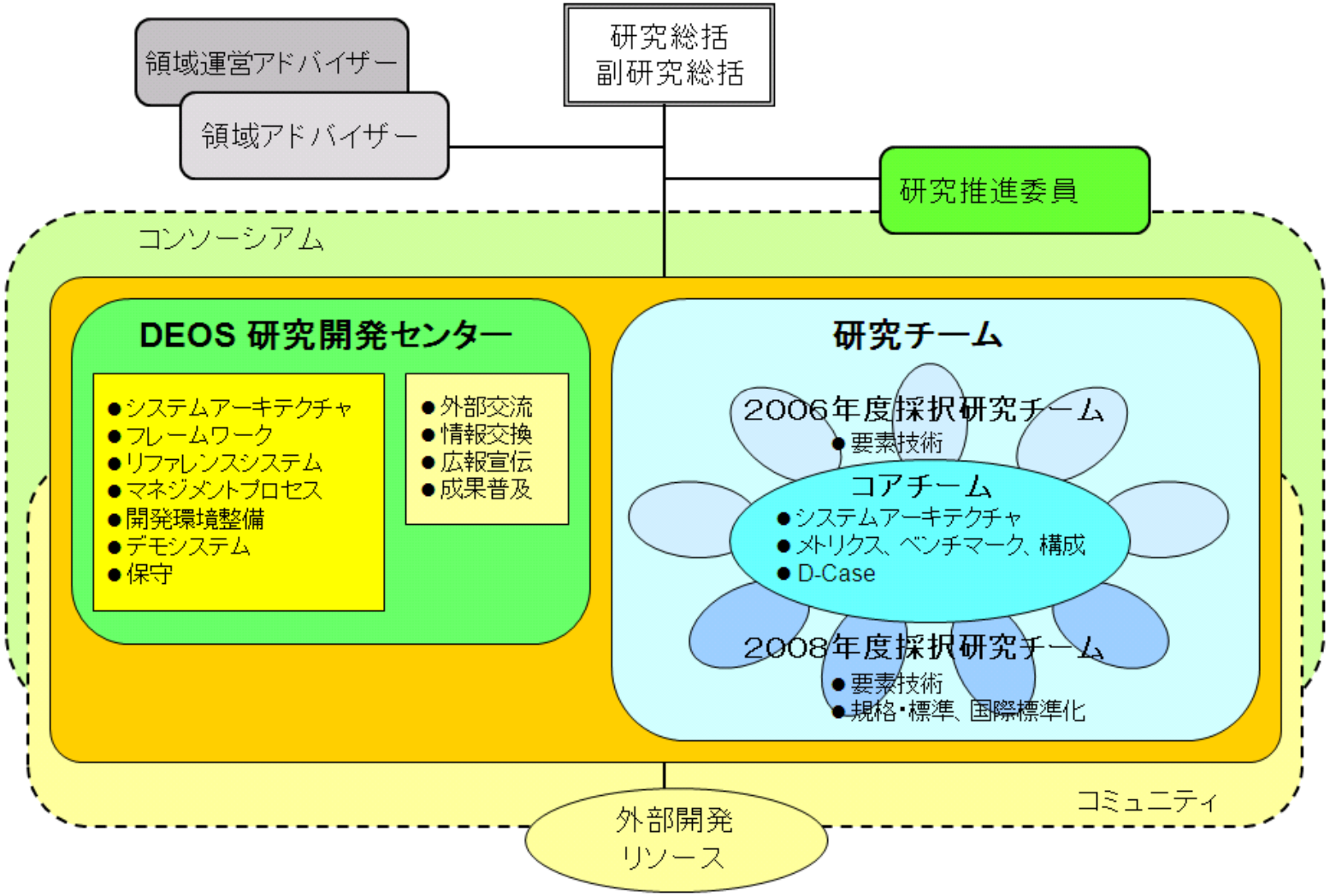
- オープンシステムディペンダビリティの観点からの組込みシステムにおける信頼性、安全性、使いやすさなどの要件の再検討

- 実用化を目指し、ディペンダブルシステムの実現に必要な概念アーキテクチャ、仕様書・実装ガイドライン、マネジメントプロセス、開発環境・ツールなどの関連基盤技術も含めた開発・評価基準作成・見える化・標準化

プロジェクトの経緯


研究開発ロードマップ
2009年9月 現在
会計年度
平成18年度
平成19年度
平成20年度
平成21年度
平成22年度
平成23年度
平成24年度
平成25年度
平成26年度
西暦
2006
2007
2008
2009
2010
2011
2012
2013
2014
フェーズ
フェーズ1
フェーズ2
フェーズ3
フェーズ4
領域活動
マイルストーン
DEOS研究開発センター開設
ホワイトペーパー第1版
フレームワークバージョン1
フレームワークバージョン2
規格制定標準化
2006年度チーム
採択
中間評価
最終評価
2008年度チーム
採択
中間評価
最終評価
コアチーム
コンソーシアム
発足

研究開発体制

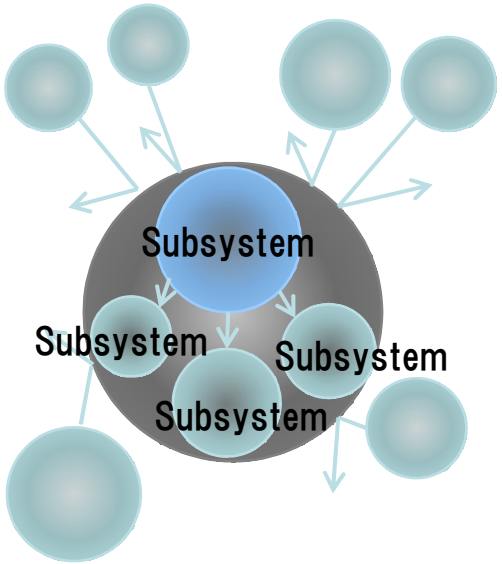

領域運営アドバイザー
領域アドバイザー
研究総括
副研究総括
研究推進委員
コンソーシアム
DEOS 研究開発センター
●システムアーキテクチャ
●フレームワーク
●リファレンスシステム
●マネジメントプロセス
●開発環境整備
●デモシステム
●保守
●外部交流
●情報交換
●広報宣伝
●成果普及
研究チーム
2006年度採択研究チーム
●要素技術
コアチーム
●システムアーキテクチャ
●メトリクス、ベンチマーク、構成
●D-Case
2008年度採択研究チーム
●要素技術
●規格・標準、国際標準化
コミュニティ
外部開発
リソース

これからのディペンダビリティ

オープンシステムディペンダビリティ

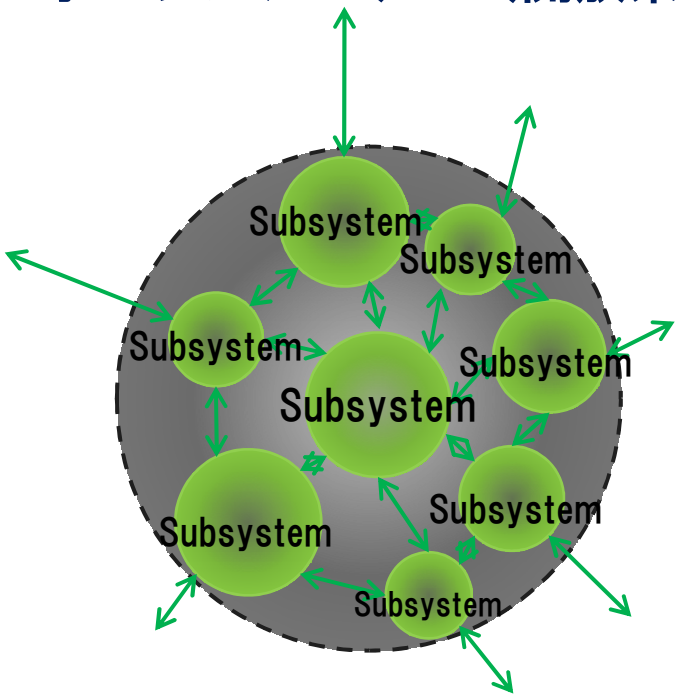
クローズドシステムとオープンシステム

クローズドシステム（閉鎖系）



- 分割して部分を理解すれば全体の問題が解決する
- 要素還元主義が成り立つ

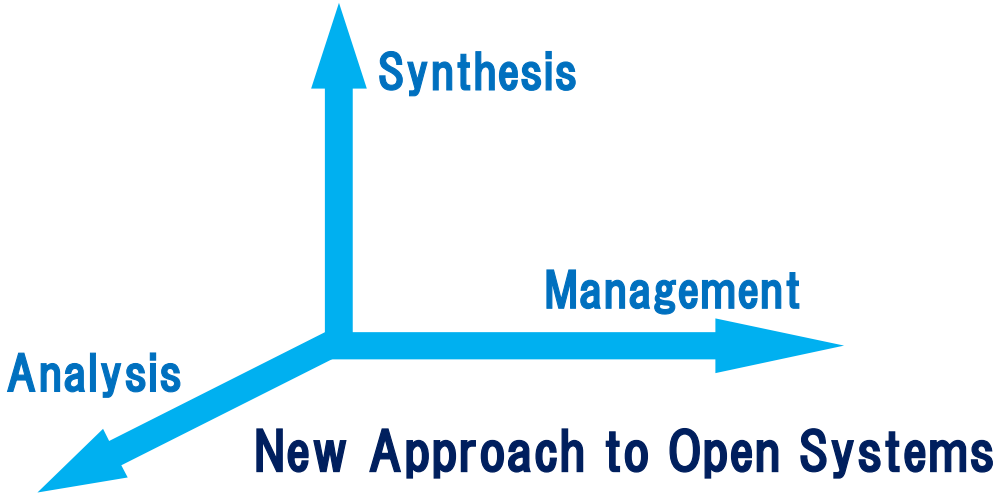
オープンシステム（開放系）



- サブシステム間の相互作用が動的に変化
- 境界領域や境界条件が動的に変化
- 定義や仕様が時間と伴に変わる
- 要素還元主義が成り立たない

オープンシステムに対処するには

- 外界に接する複雑なシステムを、生かしたまま、あるいは稼働させたまま（止めずに）問題を解決する
- サブシステムに分割しても相互依存性を保存する
- 抽象化しても捨象しない
- 「内部観測者視点」しか取りえないので、システムのモデルを現実（観測値）に一致するように常に保守する
- 「解析（Analysis)」と「合成（Synthesis)」に加えて「マネージメント（Management)」を統合・融合した新しいアプローチ



これまでのアプローチとの比較

クローズドシステムアプローチ

- 単純なシステム
- 一旦止めてもよい
- 主に平衡系
- 基本原理の解明

- 外部観測者視点
- 要素還元・抽象化が可能

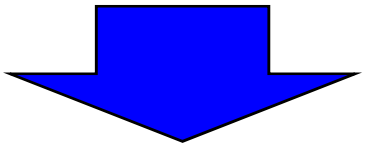
- 強力な解

オープンシステムアプローチ

- 外に開いた複雑なシステム
- 生きたまま、稼働したまま
- 時間発展系
- システムの持続性・継続性と問題の解決（多様性・一回性の理解と解決）
- 内部観測者視点
- 要素還元・抽象化が不可能、常に全体視点
- ベストエフォートによる「運営」

ライフサイクルに亘るディペンダビリティの確保はまさにオープンシステムの問題

- 仕様実装の不完全さ、システムの完全理解の困難さ
  - 要求、仕様、設計、実装、テスト仕様、テスト実施の不完全さ
  - 構成要素の論理的不透明さ（複雑化、巨大化、ブラックボックス化、レガシーコードの利用、他）
- 使用環境の変化に伴う不確実さ、システムの挙動予測の困難さ
  - 要求事項・レベルの変化、想定外の使われ方
  - ネットワークを介しての構成要素の変化、想定外の接続
  - ネットワークを介した外部からの意図的な攻撃



不完全さと不確実さを併せ持っている（開放系の特質）

オープンシステムディペンダビリティ

組込みシステムは不完全さと不確実さに起因し、未来に障害となりうる要因 （開放系障害要因）を宿命的に抱えている

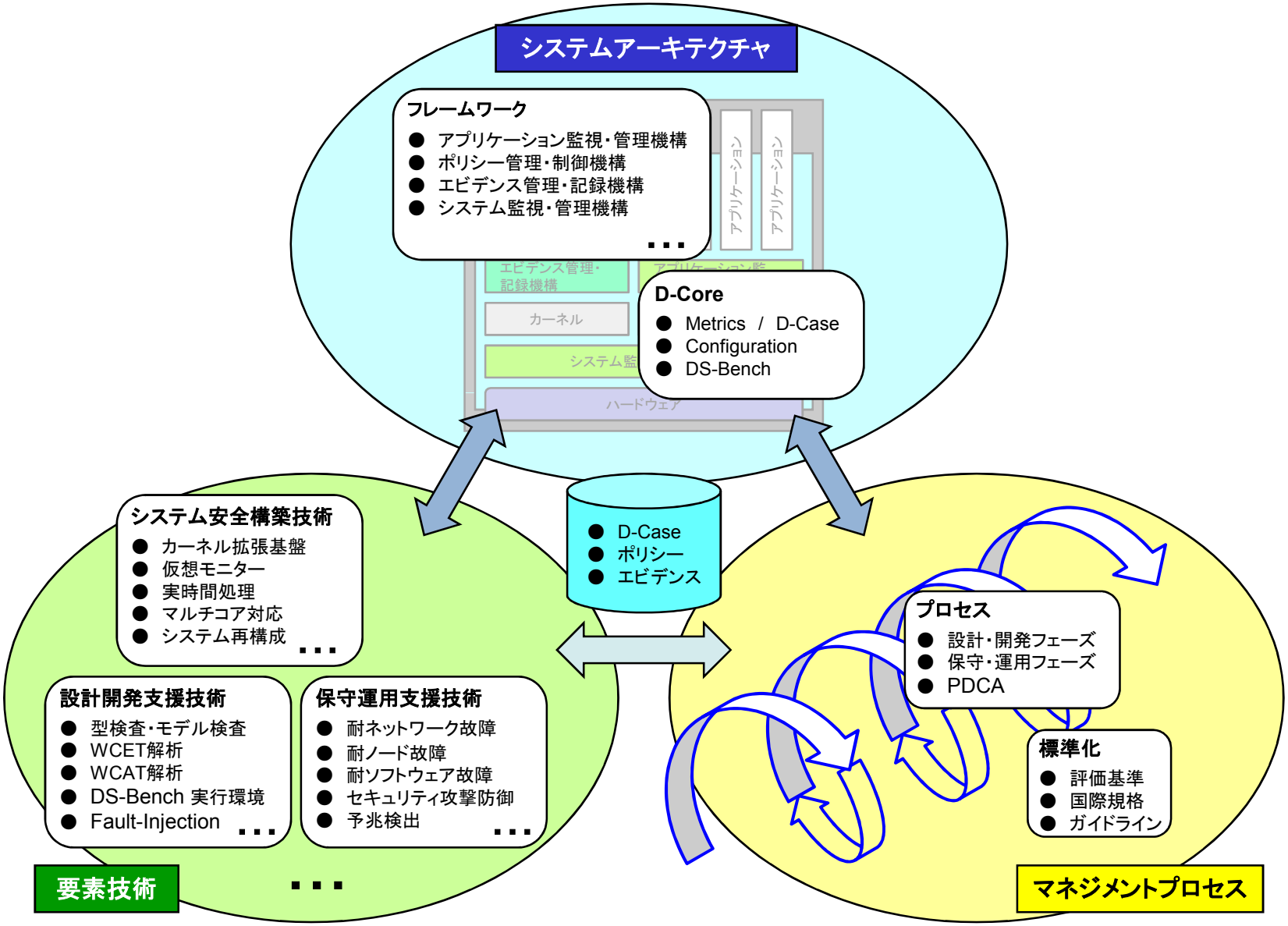
それらの要因を顕在化する前に出来る限り取り除き、また、顕在化した後に迅速かつ適切に対応し、影響を最小とするようにマネージし、利用者が期待する便益を出来る限り安全にかつ継続的に提供できること

開放系障害マネージ能力

オープンシステムディペンダビリティ向上のために

- 開放系障害を起こす要因の最小化
  - 要求、仕様、設計、実装、テストのギャップの見える化
  - 動作解析、振舞い検証
  - 動作状況の記録、説明責任マネージメント支援
  - 国際標準・規格
- 開放系障害による影響の最小化
  - 実環境・実時間での仮稼働
  - 稼働中の予知
  - 障害の最小化、迅速な復旧支援
  - 動作状況の記録、説明責任マネージメント支援

オープンシステムディペンダビリティ実現の仕組み



オープンシステムディペンダビリティの価値

- ディペンダビリティ確保のためのライフサイクルコストの低減
  - システム安全技術、設計支援技術、保守運用技術などの要素技術、システムアーキテクチャ、ならびにマネージメントプロセスにより統合的にディペンダビリティを確保し、日々改良・改善を行うことができる
- 企業の社会的責任の全うを支援
  - 障害原因ならびに回復状況の迅速な説明支援
  - 設計開発・保守運用過程の分かりやすい説明支援

今後の計画

- アーキテクチャの具体化
  - フレームワークの開発
  - D-Coreの精緻化・実装
- 要素技術の評価・改良
  - セキュリティ技術の融合
- マネジメントプロセスの確立
  - 実システムへの適用・評価
  - 規格の制定ならびに国際標準化
- 実用化
  - オープンソース化
  - コンソーシアム設立による継続的支援