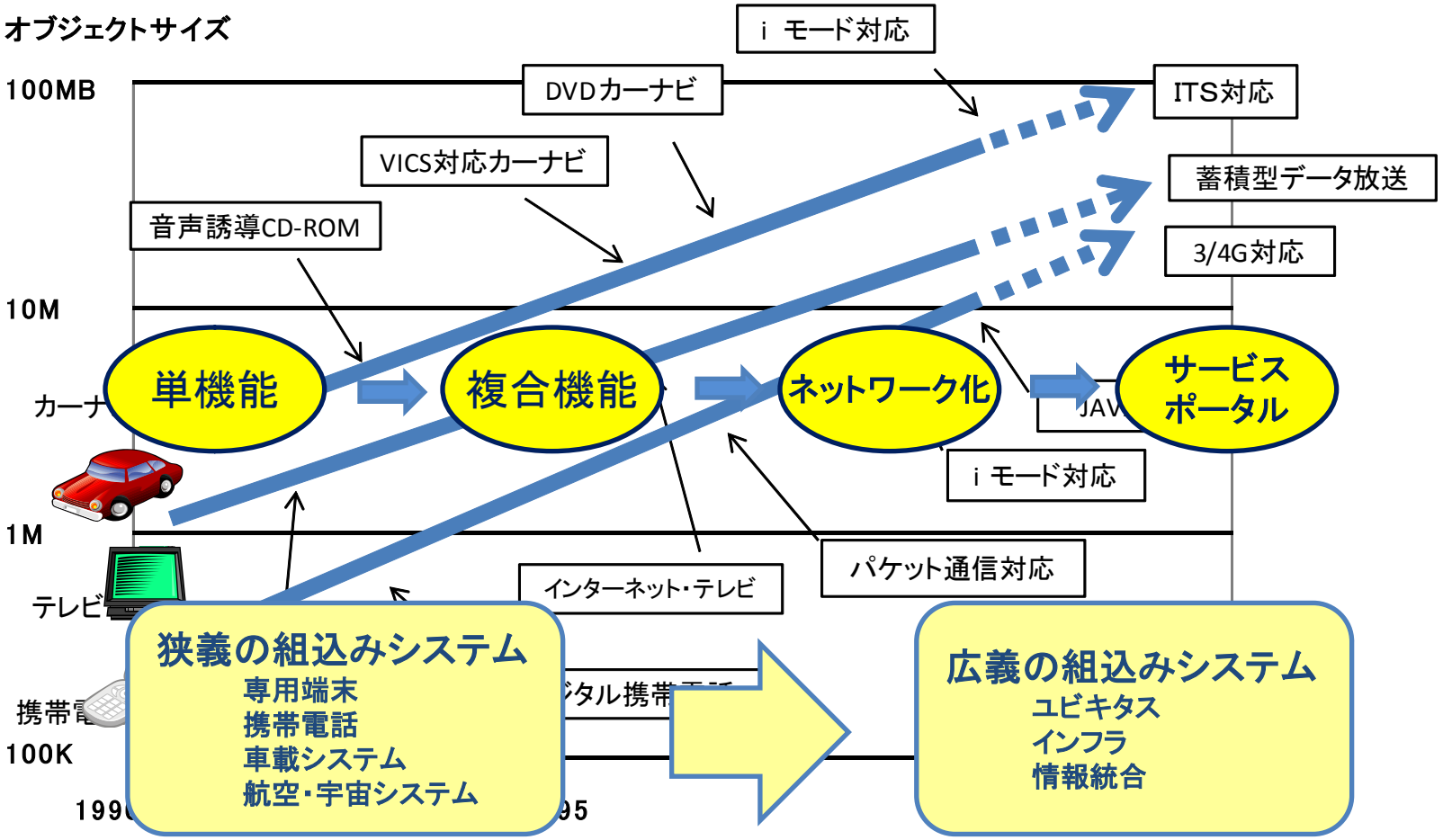
サービス継続と説明責任遂行を支えるオープンシステムディペンダビリティ

2011年11月18日
JST/CREST DEOSプロジェクト研究総括
所　眞理雄
（株式会社ソニーコンピュータサイエンス研究所代表取締役会長）

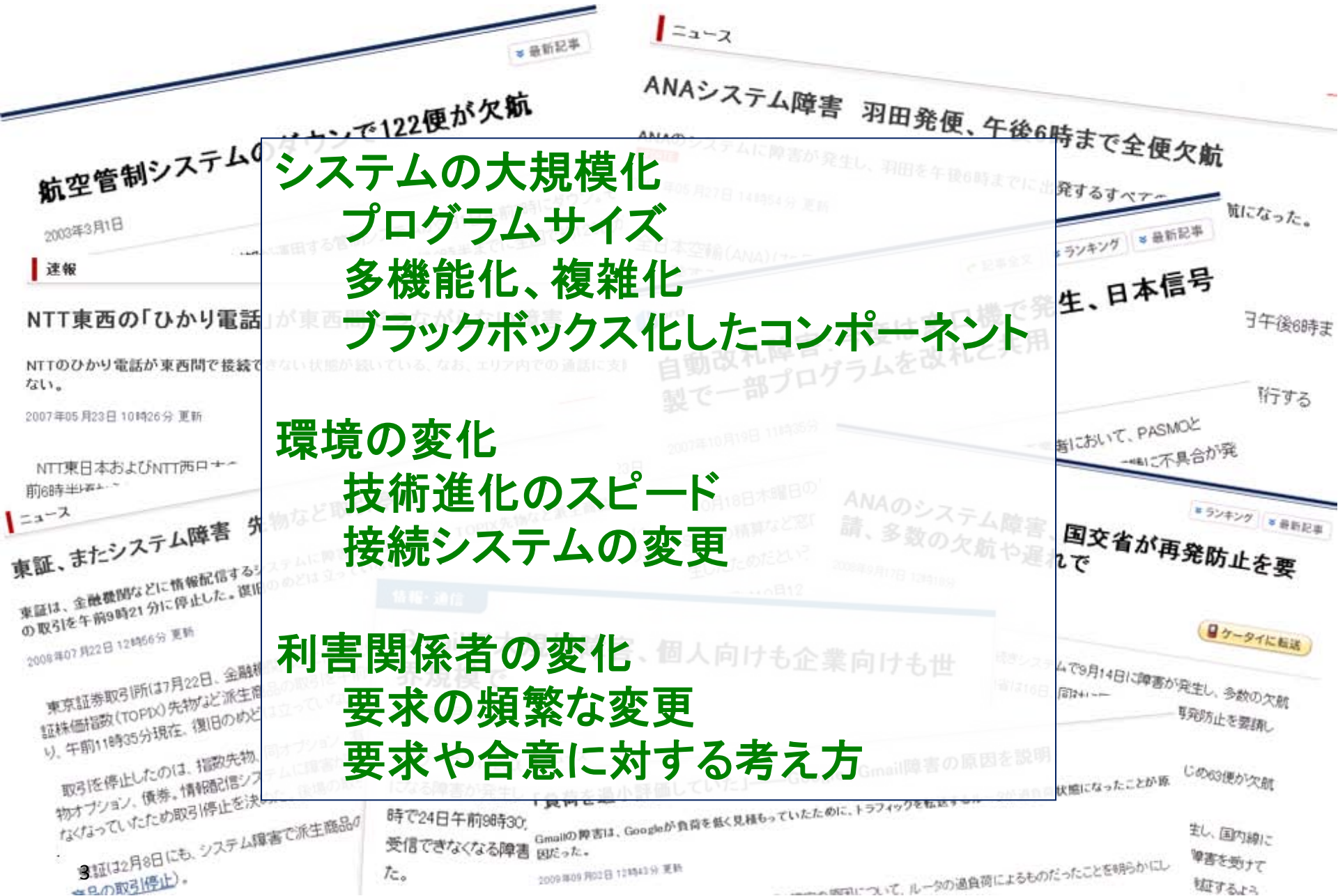
独立行政法人
科学技術振興機構
Japan Science and Technology Agency

組込みソフトウェア規模の拡大とネットワーク化



出展：日経エレクトロニクス2009.9-11（no.778）をベースに追加、修正。
経済産業省「組込みソフト産業の課題と政策展開」平成19年11月14日より

大規模なシステム障害



システムの大規模化
- プログラムサイズ
- 多機能化、複雑化
- ブラックボックス化したコンポーネント

環境の変化
- 技術進化のスピード
- 接続システムの変更

利害関係者の変化
- 要求の頻繁な変更
- 要求や合意に対する考え方

現状のまとめ

現代のコンピュータシステムは、

- システムの巨大化・複雑化
- システムのネットワーク化
- ソフトウエア部品やレガシーコードによるブラックボックス化

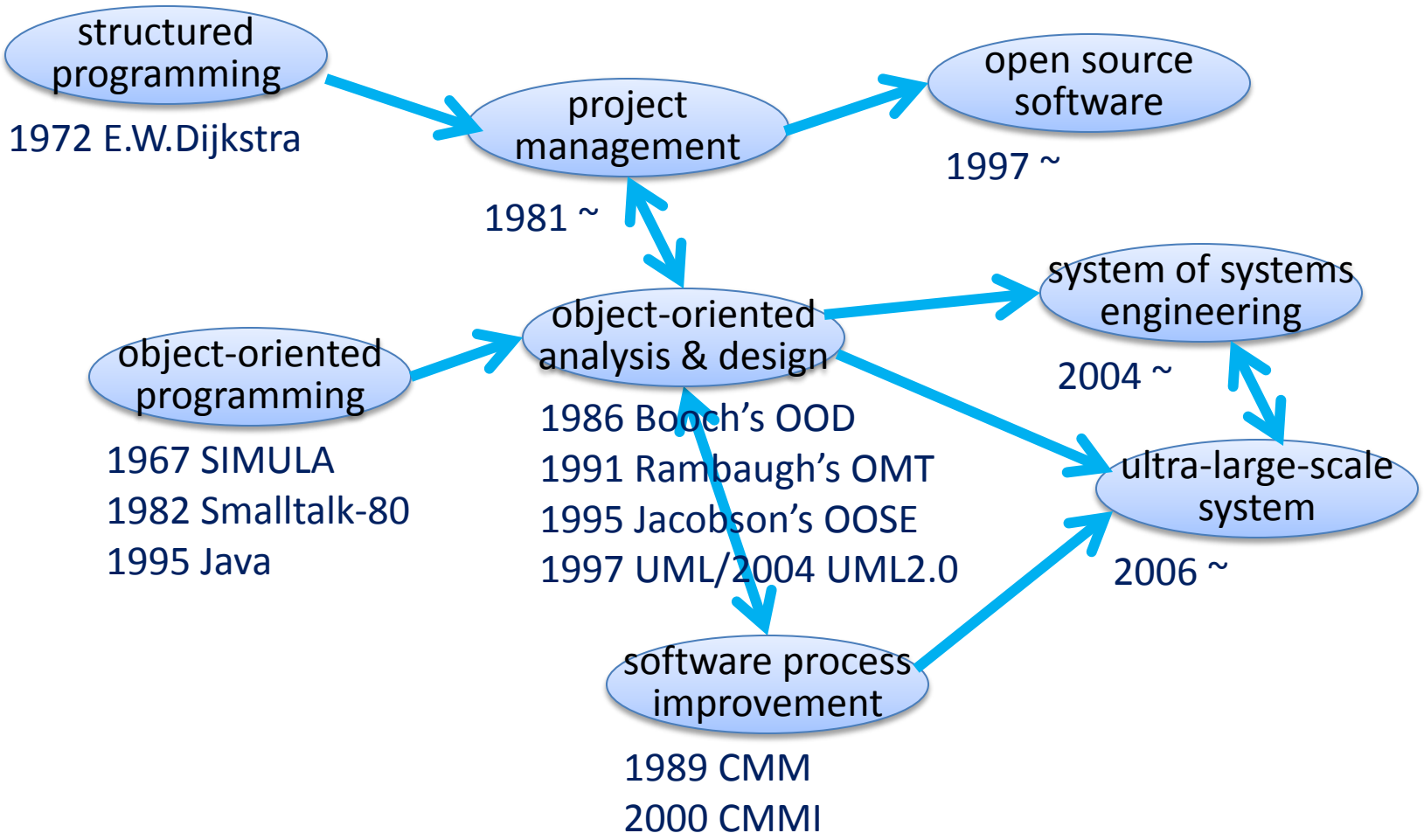
が進み、作り手ですら完全にシステムを理解し、詳細を把握し、完璧に構築する事は至難の業で、常に不完全です。

その上、

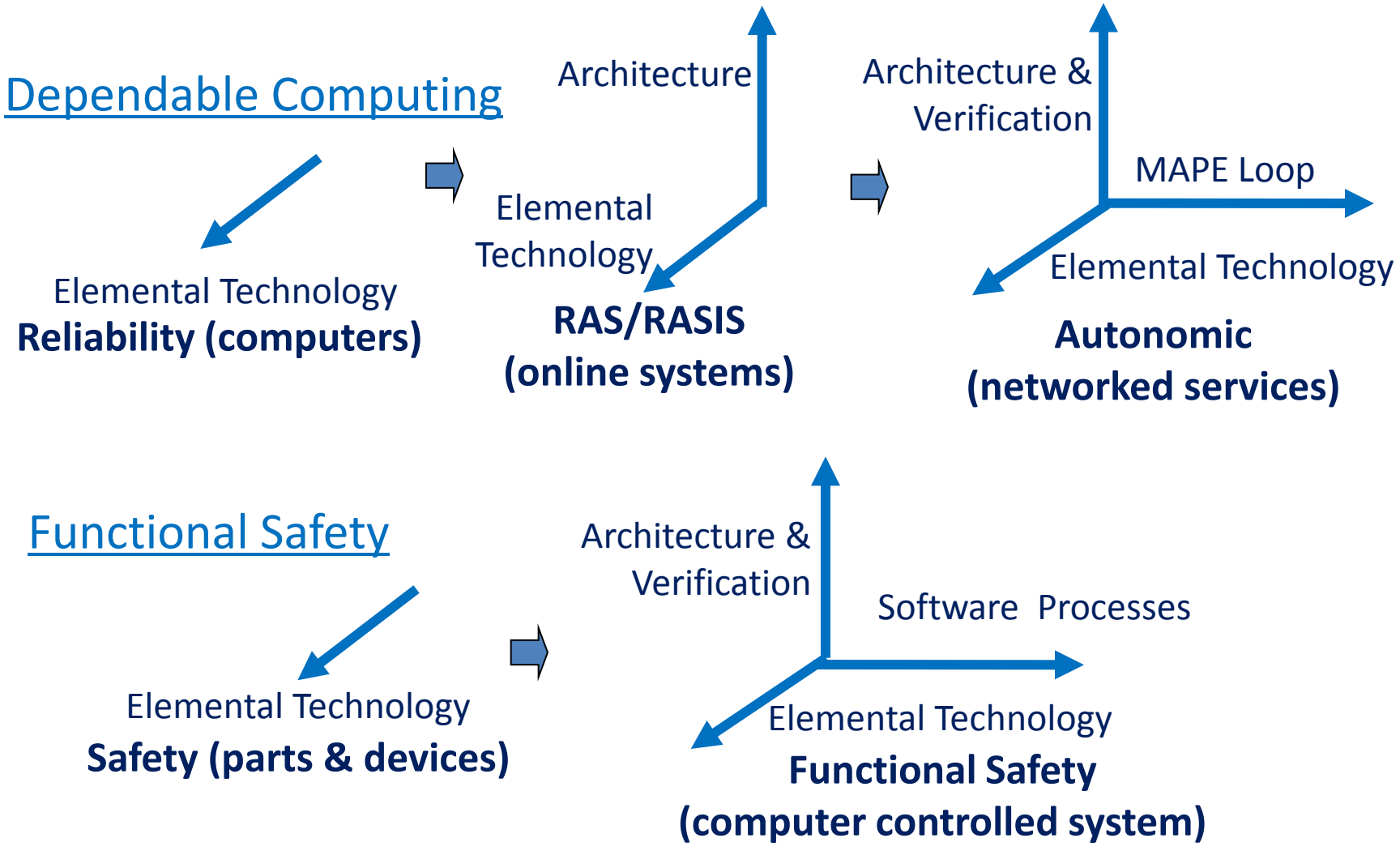
- サービス利用者の要求の変化によるサービスの多様化
- 社会のルールや仕組みの変容
- 接続されている他システムの仕様の変更

などに常にさらされ、システムの将来予測は不確実です。

ソフトウェア開発の歴史



ディペンダブルコンピューティングの歴史



ディペンダビリティーとセキュリティー（IFIP WG10.4 2004）

国際標準化

Standards

- IEC 61508: Functional Safety
- IEC 60300-1: Dependability Management
- IEC 60300-2: Dependability Program Elements and Tasks
- ISO/IEC 1207: Software Life Cycle Processes
- ISO/IEC 15288: System Life Cycle Processes
- ISO/FDIS 26262 Road Vehicles Functional Safety
- etc.

Guides

- CMMI: Capability Maturity Model Integration
- DO-178B: Software Considerations in Airborne Systems and Equipment Certification
- MISRA-C: Guidelines for the Use of the C Language in Vehicle Based Software
- IEC 61713: Software Dependability through the Software Life-Cycle Processes – Application Guide
- IEC 62347: Guidance on System Dependability Specifications
- etc.

産業界主導のデファクト標準化

- AUTOSAR for Automotive
- HIDENETS for Automotive
- ARINC 653 for Aerospace and Defense
- Solaris 10, Linux RAS, and Autonomic Computing for Enterprise Systems
- Carrier Grade Linux and Service Availability Forum for Communication/Network Operators
- Open Group / TOGAF
- etc.

オープンシステムディペンダビリティー

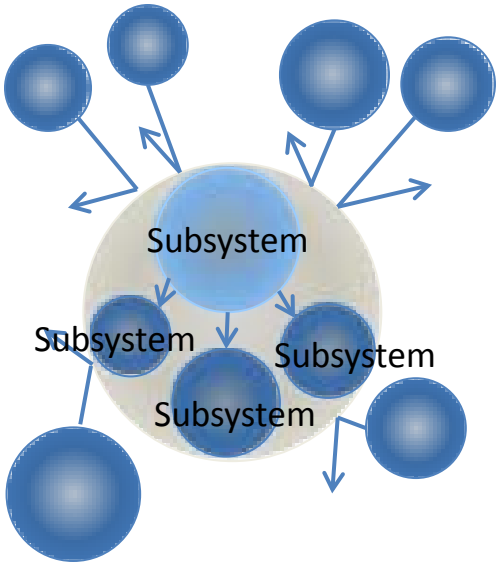
すなわち、現代のコンピュータシステムは機能、構造、システム境界が時間的に変化しつづけるオープンシステム（開放系）であり、これに起因する不完全さと不確実さを完全に排除することができず、未来に障害となりうる要因（開放系障害要因）を本質的に抱えています。

私たちは、それらの要因を顕在化する前にできる限り取り除き、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できる限り安全にかつ継続的に提供する努力、社会への責任ある説明、およびそれらを継続的に行うことが必要だと考えています。

私たちはこの能力を「オープンシステムディペンダビリティー（Open Systems Dependability）」と呼び、これを実現するための知識・技術体系を「DEOS：オープンシステムのためのディペンダビリティ工学（Dependability Engineering for Open Systems ）」と名付けました。

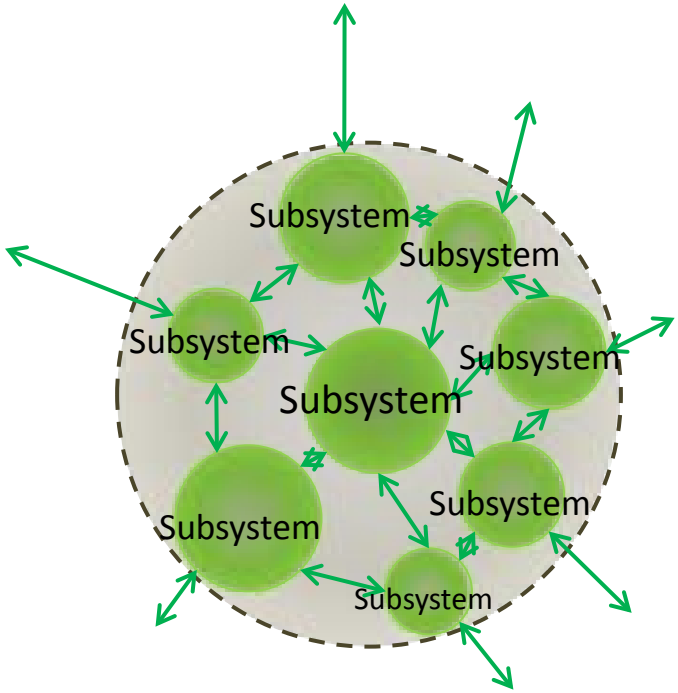
オープンシステムとは何か？

クローズドシステム（閉鎖系）



- 境界領域や境界条件が不変
- 定義や仕様が一定
- 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

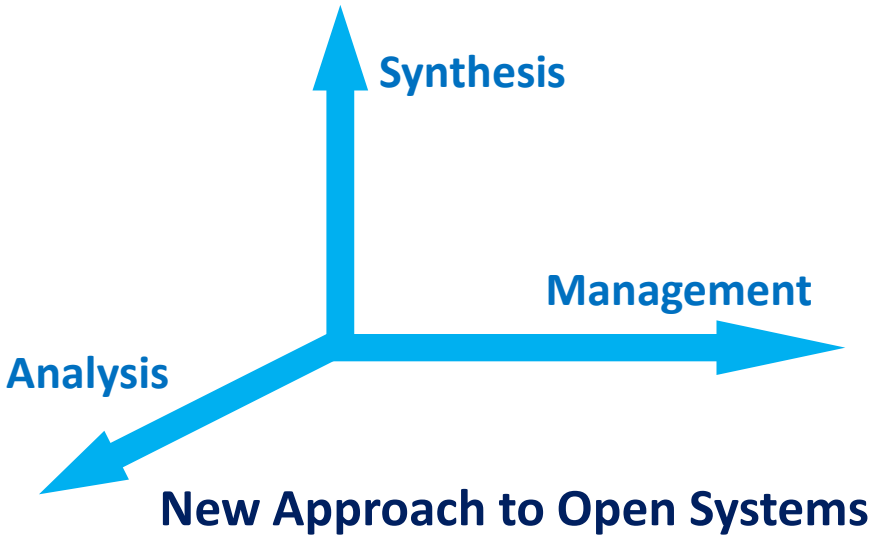
オープンシステム（開放系）



- 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
- サブシステム間の相互作用が動的に変化
- 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
- 「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



サービス継続と説明責任の全う

我々は、「変化しつづけるシステムのサービス継続と説明責任の全う」のためにはオープンシステムディペンダビリティーの実現が必須であると考えています。そして、そのためには、

- ✓ 継続的な改良改善のための反復的なプロセス（DEOS プロセス）
- ✓ これを仕組みとして支えるアーキテクチャ（DEOSアーキテクチャ）
- ✓ 仕組みを実行する構成要素プロセス群・要素技術群

私たちは、DEOSを実践する事の究極のメリットは次の３点であると考えます。

- ◆ エンドユーザーのサービス享受の権利を護る
- ◆ サービス提供者のビジネス（ブランド）を護る
- ◆ サービス提供経営陣が社会的義務を果たす

DEOSの特徴

DEOSの特徴は「**DEOSプロセス**」と、これを効率よく実現するための「**DEOSアーキテクチャ**」によるディペンダビリティの達成にある

- **DEOSプロセス**：オープンシステムディペンダビリティの実現のためのプロセス
  - ✓ **反復的アプローチ**
  - ✓ **プロセスのプロセス**

  目的や環境の変化に対してシステムを継続的に変更して行くための変化対応サイクルと、障害に対して迅速に対応するための障害対応サイクルからなる

- **DEOSアーキテクチャ**：DEOSプロセスを支援する仕組み
  - ✓ **要求マネジメントプロセスを支えるツールや合意記述データベース**
  - ✓ **ディペンダブルなソフトウェアを開発するためのツール群**
  - ✓ **システムの監視・記録や障害時の迅速対応を担う実行環境**

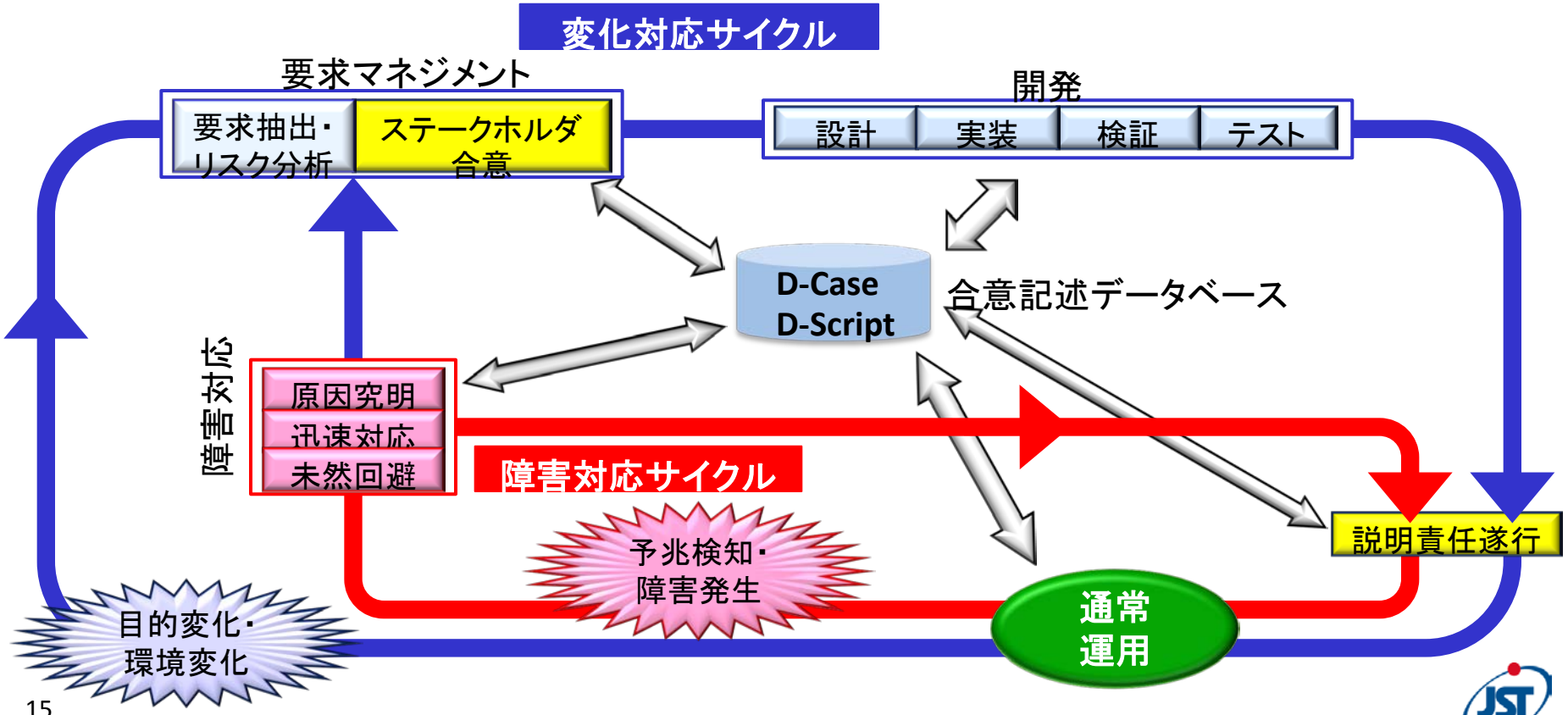
  具体的にはD-Case/D-Case ツール、プログラム開発ツール、DEOSランタイム環境（DEOS Runtime Environment = DRE）、D-Scriptなどから構成される

DEOSプロセス

オープンシステムディペンダビリティの実現のためのプロセス

◆反復的アプローチ
- 目的や環境の変化に対してシステムを継続的に変更して行くためのサイクル
- 障害に対して迅速に対応するためのサイクル

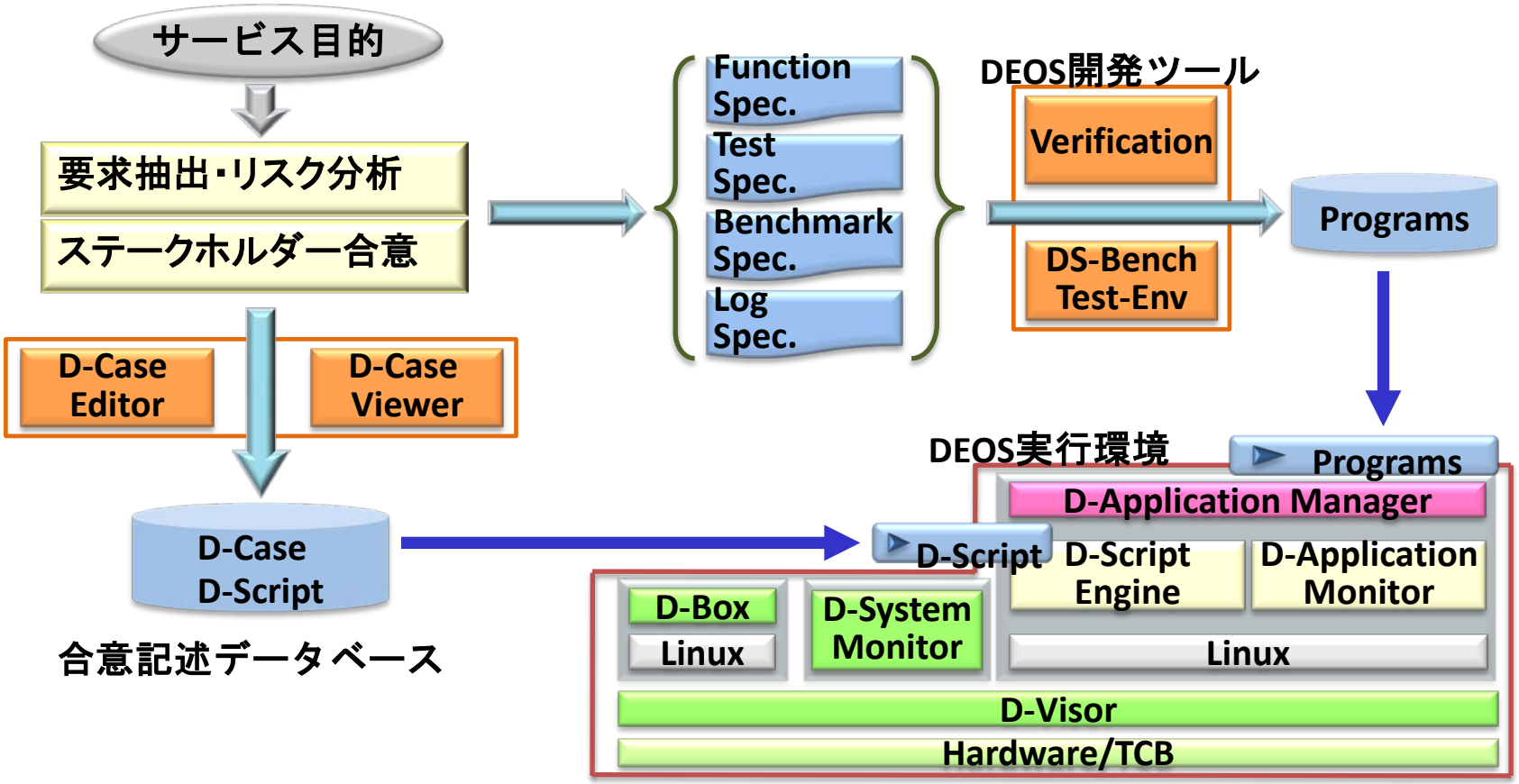
◆ プロセスのプロセス
- 相互に有機的に結びつけられた構成要素プロセス



DEOSアーキテクチャー

DEOSプロセスを支援する仕組み

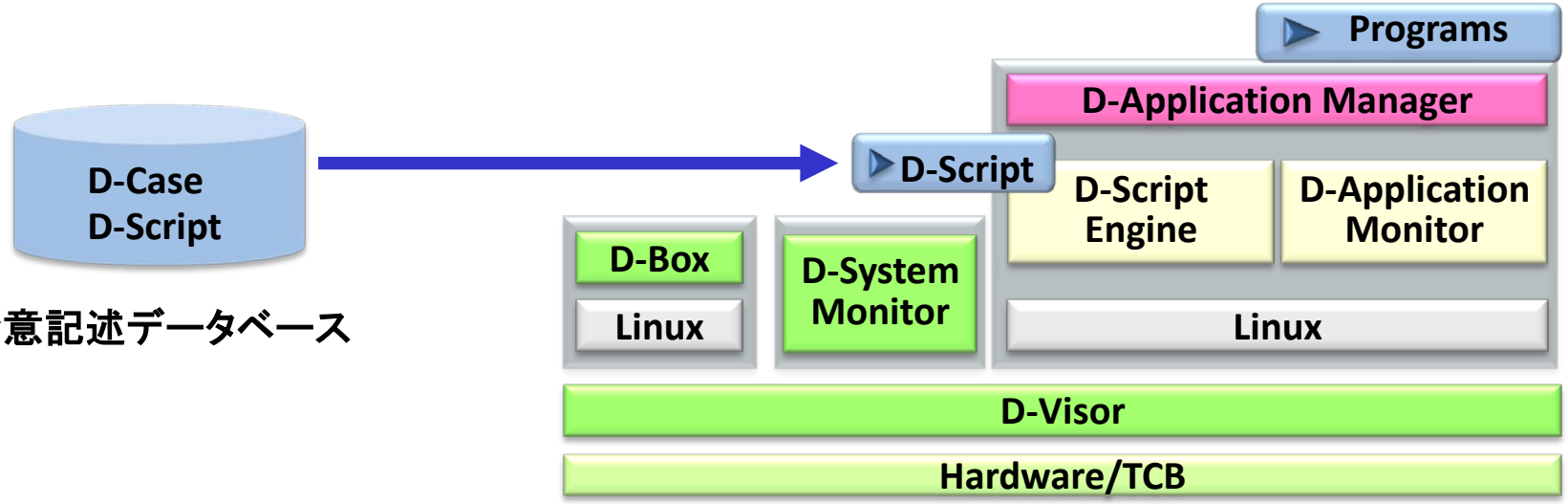
- 要求マネジメントプロセスを支えるツールや合意記述データベース
- ディペンダブルなソフトウェアを開発するためのツール群
- システムの監視・記録や障害時の迅速対応を担う実行環境



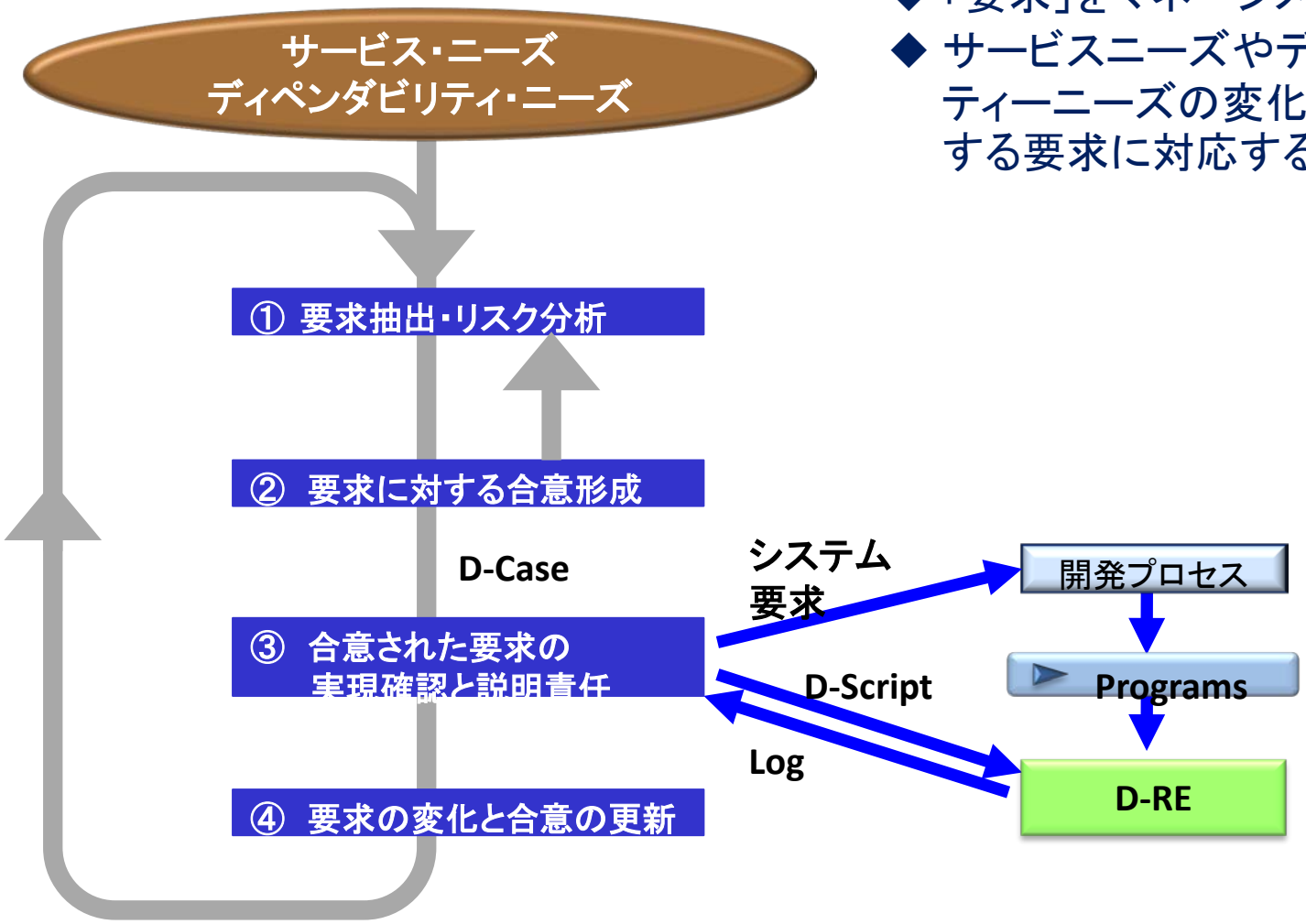
DEOS実行環境(D-RE)

DEOS実行環境の構成

- D-Application Manager: アプリケーションコンテナーを提供する
- D-Application Monitor: アプリケーションの動作を監視し、ログを収集する
- D-System Monitor: システムの動作を監視し、ログを収集する
- D-Script: いつ、どのようなログを収集するか、どのように故障に対処するかを指示するシナリオが書かれている
- D-Script Engine: D-Scriptを安全・確実に実行する
- D-Box: 収集されたログを格納する
- D-Visor: ハードウエアを抽象化し、システムコンテナーを提供する



DEOSプロセスにおける要求マネージメント



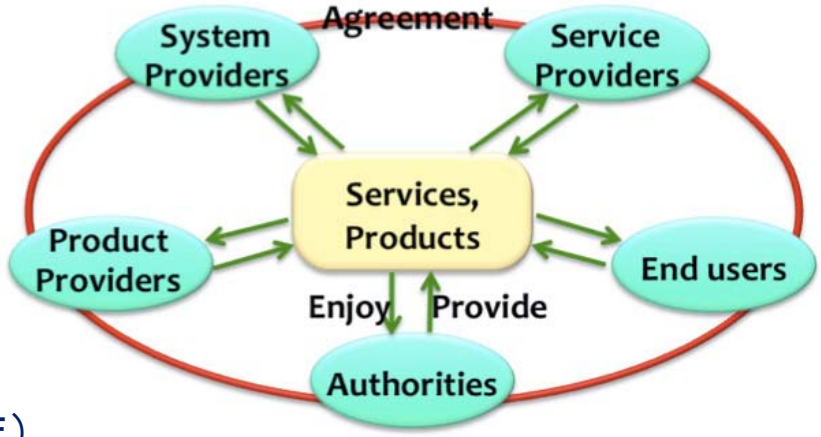
DEOSにおける要求マネージメント

- 「要求」をマネージメントの単位とする
- サービスニーズやディペンダビリティーニーズの変化に対応し、変化する要求に対応する

要求に対するステークホルダー合意の形成

ステークホルダー

- サービス・製品の利用者（潜在的ステークホルダー）
- サービス・製品の提供者（事業主）
- システム提供者
  - 設計開発者
  - 保守運用者
  - ハードウェア供給者
- サービス・製品認可者（規制監督官庁）



合意の形成

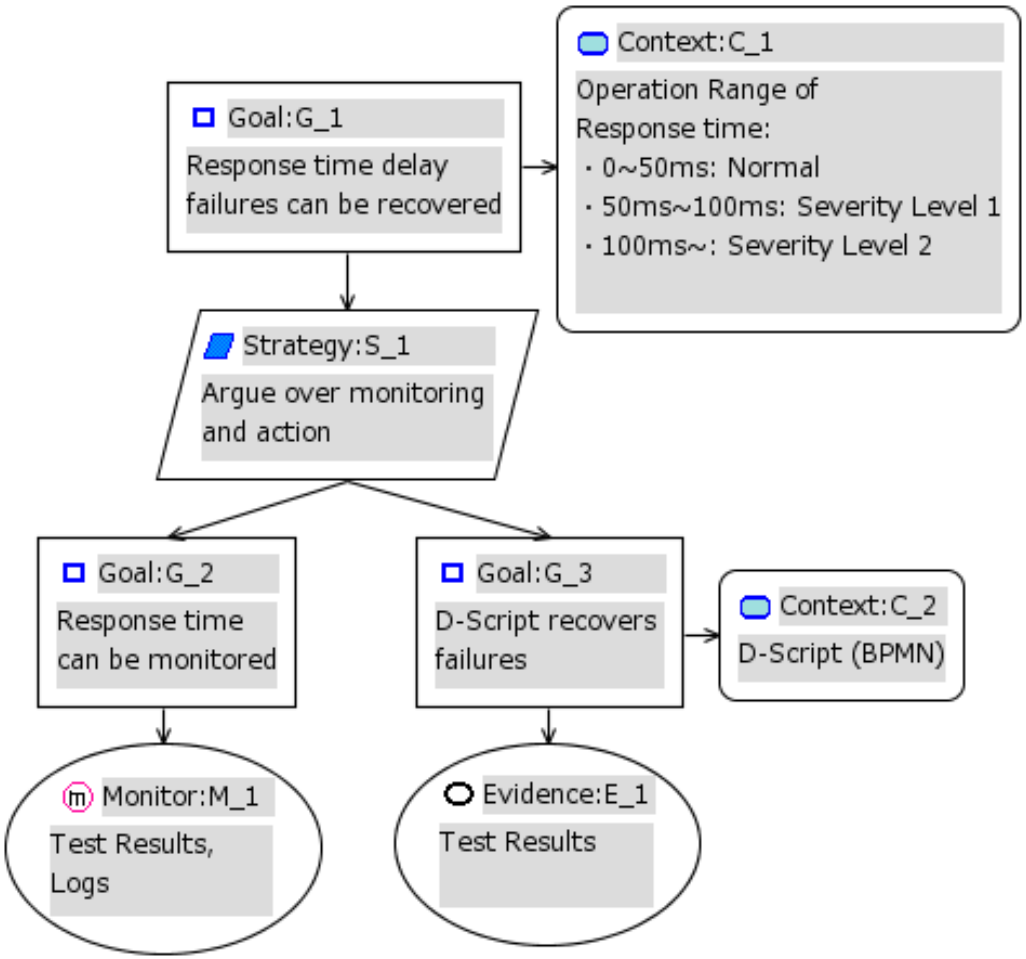
合意の形成はD-Caseを用いて行う。D-CaseはGSN(Goal Structureing Notation)を基にしており、以下の特徴を持つ

- 議論とエビデンスに基づく合意のための、構造化された表記法
- ステークホルダ間合意のマネージメントサポート
- 通常運用時におけるステークホルダ間合意のモニタリングサポート(モニタノード)
- 合意内容記述の整合性検査サポート

D-CASE記述の例

サーバの応答遅延障害に関する議論内容を表した例

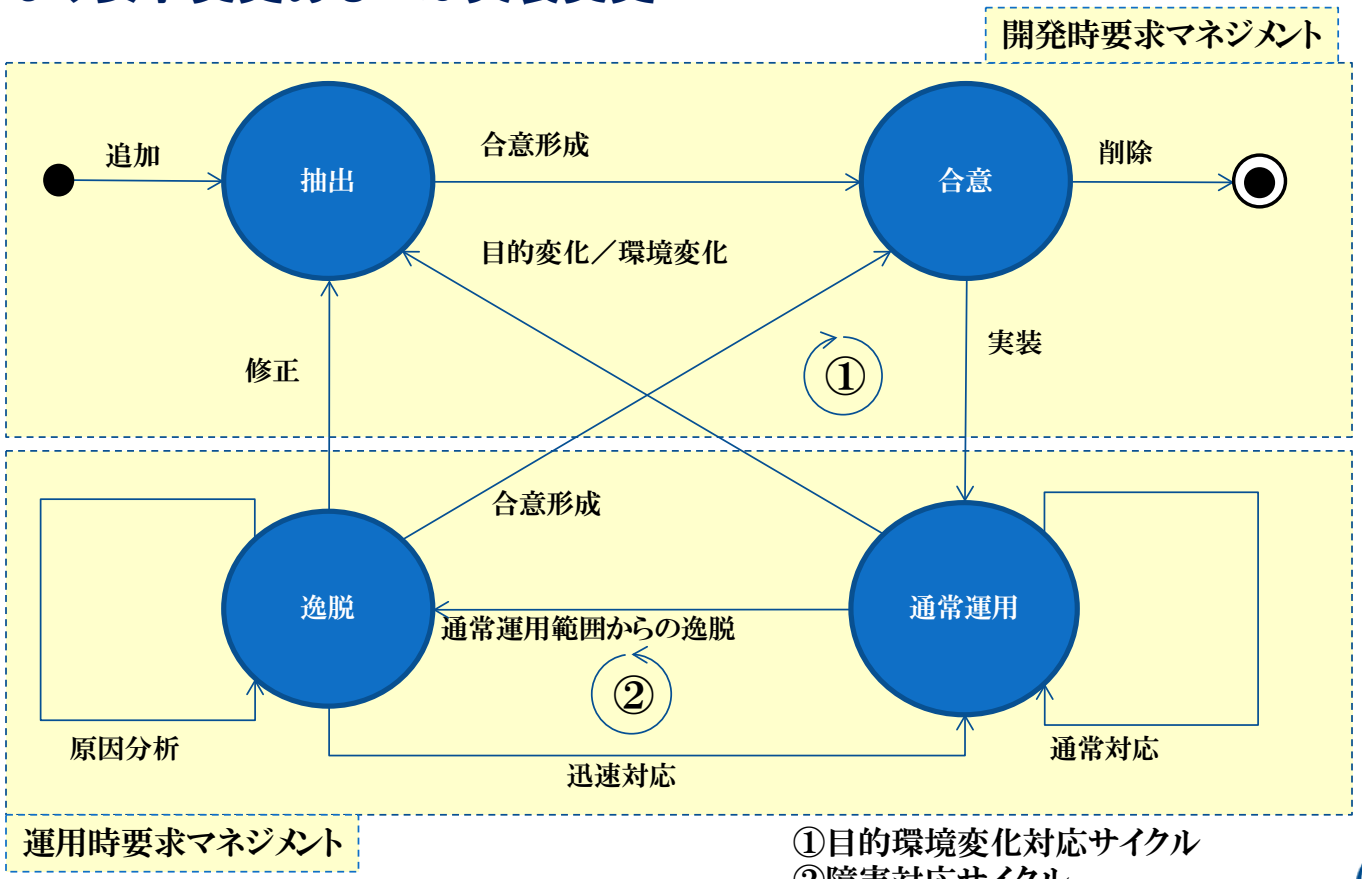
- コンテキストノードC_1に応答時間の変動許容範囲(0~50ミリ秒)と、変動許容範囲を超えた場合の深刻度(1および2)が定義されている。
- このD-Caseは、サーバの応答時間を常にモニタリングできることを、モニタリングノードM_1により保証し、
- 応答時間が変動許容範囲を超えた場合、深刻度に応じて、D-Scriptにより、応答時間を変動許容範囲に戻せることを、事前のテスト結果によるエビデンス(E_1)により保証している。



要求の変化と合意の更新

要求の状態によるマネージメント

- 要求の抽出、合意の形成、通常運用
- 目的変化・環境変化による要求の変化
- 通常運用範囲からの逸脱
  - 迅速対応により通常運用に復帰
  - 修正により要求変更あるいは実装変更



①目的環境変化対応サイクル
②障害対応サイクル

D-SCRIPTによる柔軟な制御

D-ScriptはD-Caseの記述を基にアプリケーションプログラムを動的に制御する

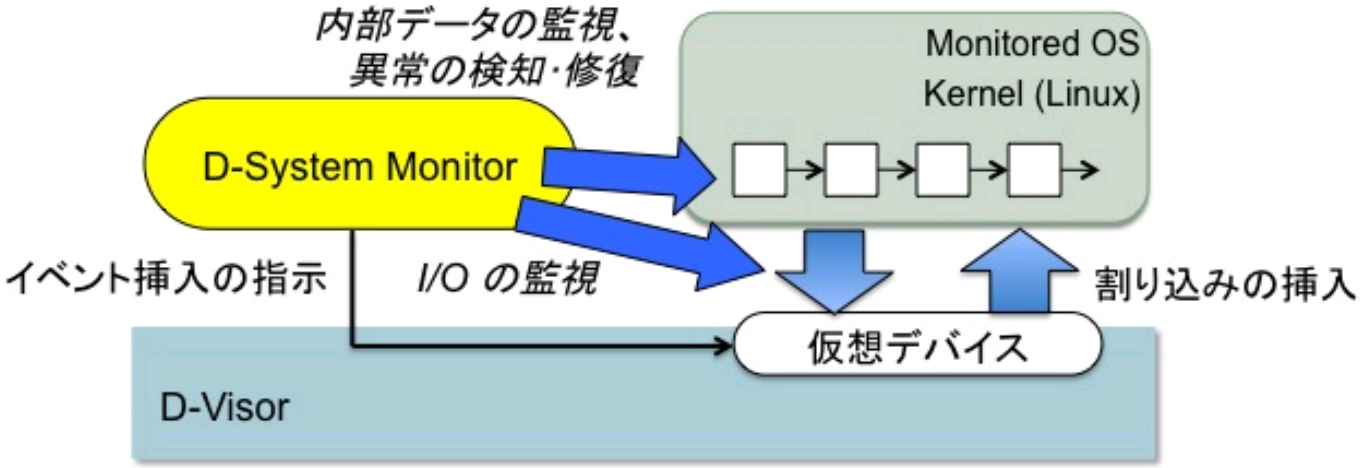
- D-Script： D-Scriptシナリオの集合
- D-Scriptシナリオ： D-Script Engineが実行するD-TaskとD-Controlからなるひとまとまりの処理
- D-Task： 処理の基本単位
- D-Control： 逐次実行、分岐処理、並列実行の指示

D-Script シナリオ

起動

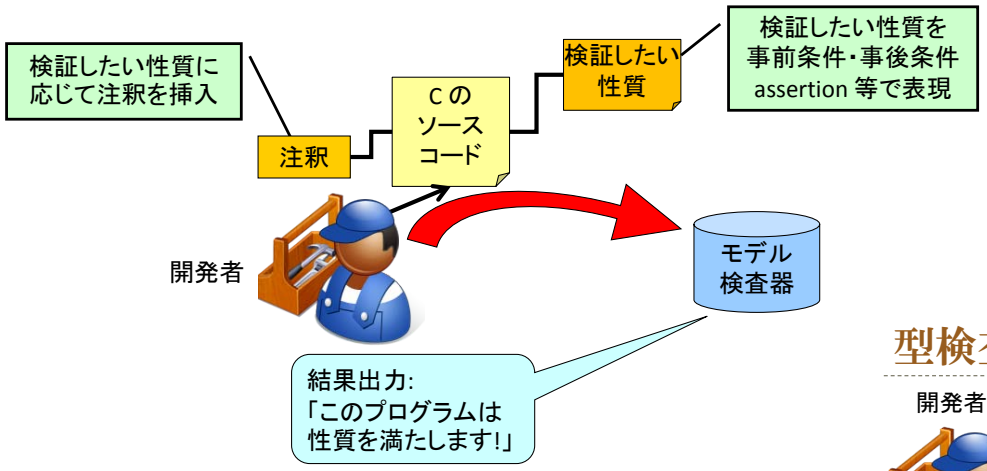
DEOSセキュリティー機構

- OS カーネルを監視して、OS カーネルが提供する
  セキュリティ機構が期待通り動作しているかを調べる
  - OS カーネルが乗っ取られると、その上で動作する
    セキュリティ機構は信頼できない



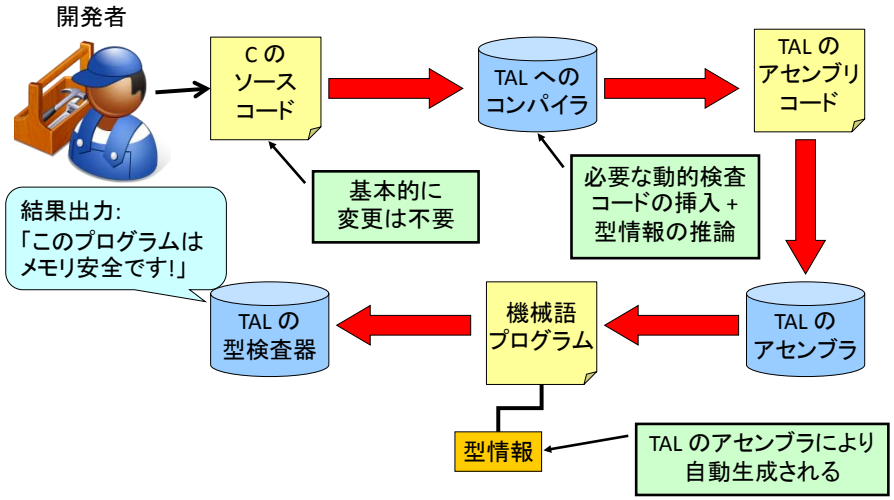
- 様々なイベントを OS カーネルに挿入してその反応を監視する
  - 異常な振る舞いを検知したら、OS が乗っ取られていると判断
    - イベント: 割り込みの挿入、システムコール列の挿入など
    - 反応: デバイス I/O や制御レジスタへのアクセス，OS の内部データ構造の動き

モデル検査の概要



モデル検査では、Cプログラムの実行パスを網羅的に探索し、開発者によって指定された性質(条件)が満たされたかどうかを検査する。

型検査の概要

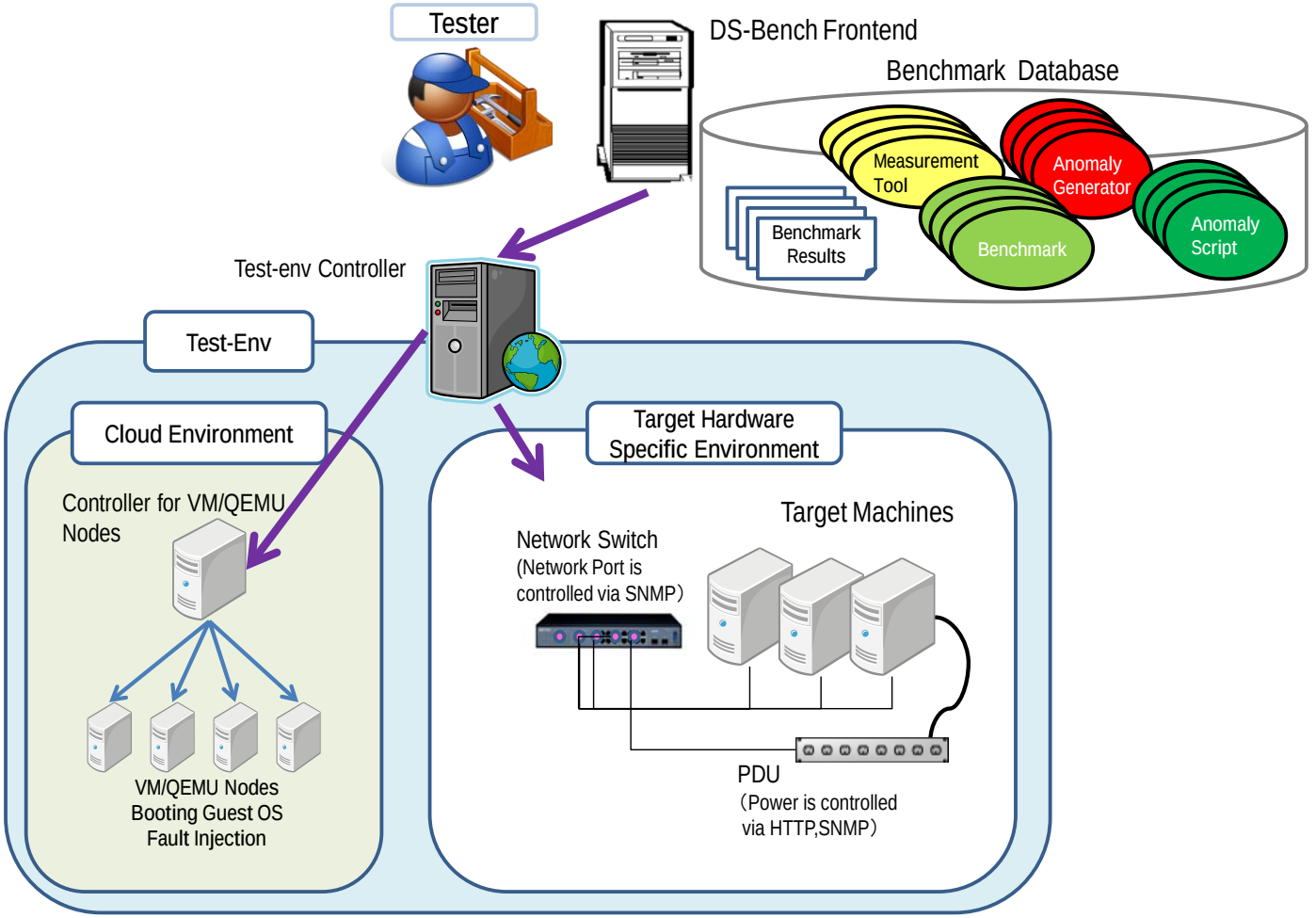


型検査では、プログラムが不正なメモリ操作を行わないことを検査して保障する。

TAL (= 型付きアセンブリ言語)
アセンブリ言語・機械語のレベルで型検査が可能

ディペンダビリティー・テスト支援ツール

DS-Bench:　ベンチマーク実行・フォールトインジェクションテストの実行
TEST-Env:　ベンチマークやテストの実行環境となるハードウェア資源の管理と制御



国際標準化

国際標準化の重要性

- オープンシステムディペンダビリティー概念の共有
- システムのディペンダビリティーに関する社会的な仕組みの構築
- 標準ツールの普及

策定を目指す規格

- オープンシステムディペンダビリティー概念規格
  - IEC60300　IEC TC56/NWIP
- 合意形成と説明責任の方法論、プロセス規格
  - ISO/IEC15026　System and Software Assurance
  - ICE TC56、OMG
- エンタープライズアーキテクチャとディペンダビリティー
  - Open Group　OMG、TOGAF

DEOSコンソーシャム

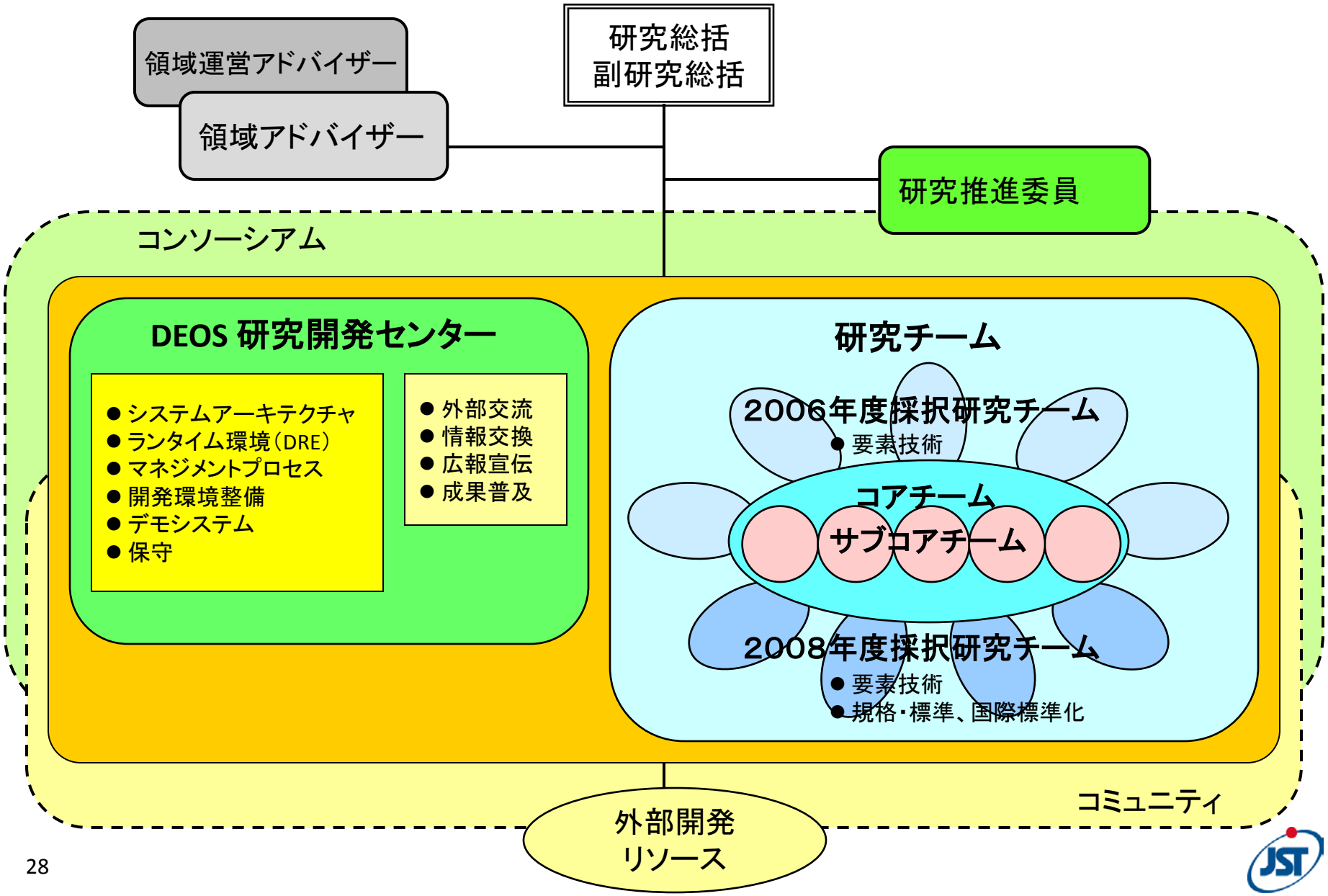
DEOSコンソーシャムの目的

- オープンシステムディペンダビリティの重要性の理解・世論形成の推進
- 業界あるいは社会にまたがる標準作成
- 業界あるいは適用分野別のDEOSプロセスおよびアーキテクチャ適用支援
- オープンシステムディペンダビリティに関連した産業の育成
- DEOSに関連した成果物の開発・維持

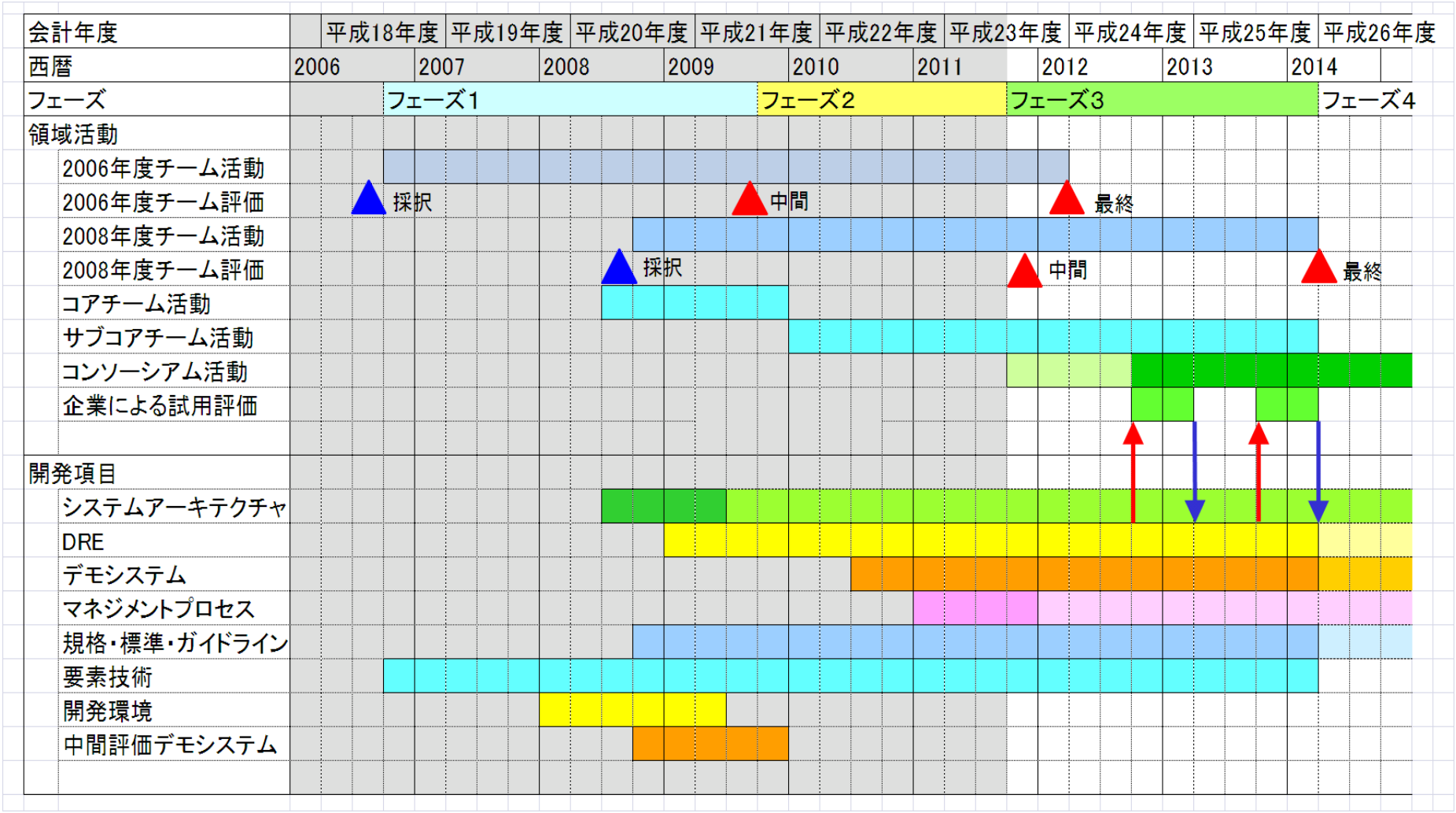
DEOSコンソーシャム設立計画

- 2011年11月　設立準備会発足
- 2012年あるいは2013年　DEOS国際コンソーシャム設立

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
● ランタイム環境（DRE）
● 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
サブコアチーム
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

ロードマップ


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
2006年度チーム活動
2006年度チーム評価
採択
中間
最終
2008年度チーム活動
2008年度チーム評価
採択
中間
最終
コアチーム活動
サブコアチーム活動
コンソーシアム活動
企業による試用評価
開発項目
システムアーキテクチャ
DRE
デモシステム
マネジメントプロセス
規格・標準・ガイドライン
要素技術
開発環境
中間評価デモシステム

まとめ

- Open Systems Dependability実現のための研究・開発
- 実用化につながる研究と開発
  - ニーズの強い、新しい研究開発分野を創造する
  - 日本の産業の活力・世界的な地位向上につながる
- 領域をあげての統合された成果
  - 分野ごとに従来の研究を進めるのではなく、統合された大きな成果
  - 新たな学問領域へのチャレンジ
- 世界の標準へ
  - 実用化のための必要条件
  - ディペンダビリティ技術の標準化による安心・安全な社会への貢献
- コンソーシアム設立
  - 実用化に必要な保守の確保
  - 成果の活用・保守・標準化

主たる研究者

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　センター長・教授
	佐藤　三久	筑波大学 計算科学研究センター センター長
	徳田　英幸	慶應義塾大学 環境情報学部　教授
	中島　達夫	早稲田大学 理工学術院　教授
	前田　俊行	東京大学 大学院情報理工学系研究科　助教
平成20年度採択 研究代表者		
	加賀美　聡	独立行政法人 産業技術総合研究所デジタルヒューマン工学研究センター　副センター長
	木下　佳樹	独立行政法人 産業技術総合研究所　情報技術部門　主幹研究員
	倉光　君郎	横浜国立大学 大学院工学研究院 准教授
	河野　健二	慶應義塾大学 理工学部　准教授

研究推進委員

浅井　信宏	日本アイ･ビー･エム株式会社 ソフトウェア開発研究所 ディスティングイッシュト･エンジニア
大野　毅	横河電機株式会社　IA技術開発事業部　ネットワークテクノロジ部　組込基盤課　課長
中川　雅通	パナソニック株式会社　システムエンジニアリングセンター　オープンシステムエンジニアリンググループ　グループマネジャー
森田　直	ソニー株式会社 CPDG･プロフェッショナル･ソリューション事業本部 Felica事業部 要素技術開発部　統括部長
山浦　一郎	富士ゼロックス株式会社 コントローラ開発本部 コントローラプラットフォーム第2開発部　グループ長
横山　和俊	株式会社NTTデータ 技術開発本部　課長

WHITE PAPER 執筆者

White Paper 第3版が出版されました。DEOSセンターのホームページからダウンロード可能になります。 Whitepaper執筆者は以下の通りです。

- 科学技術振興機構・・・小野　清志、 高村　博紀、 松原　茂、 宮平　知博、 屋代　眞
- 慶應義塾大学・・・・・河野　健二、 徳田　英幸、 中澤　仁、 山田　浩史
- 産業技術総合研究所・・石綿　陽一、 加賀美　聡、 木下　佳樹、 高井　利憲、 武山　誠、 田口　研治
- ソニーコンピュータサイエンス研究所・・・・・・所　眞理雄
- 筑波大学・・・・・・・・追川　修一、 佐藤　三久、 塙　敏博、 朴　泰祐
- 東京大学・・・・・・・・石川　裕、 藤田　肇、 前田　俊行、 松野　裕、 横手　靖彦
- 名古屋大学・・・・・・山本　修一郎
- 横浜国立大学・・・・・倉光　君郎、 菅谷　みどり
- 早稲田大学・・・・・・中島　達夫

ご清聴ありがとうございました

引き続きご支援をよろしくお願いします

JST/DEOS Project
http://www.jst.go.jp/kisoken/crest/ryoiki/bunya04-4.html

JST/DEOS Center
http://www.dependable-os.net/index.html