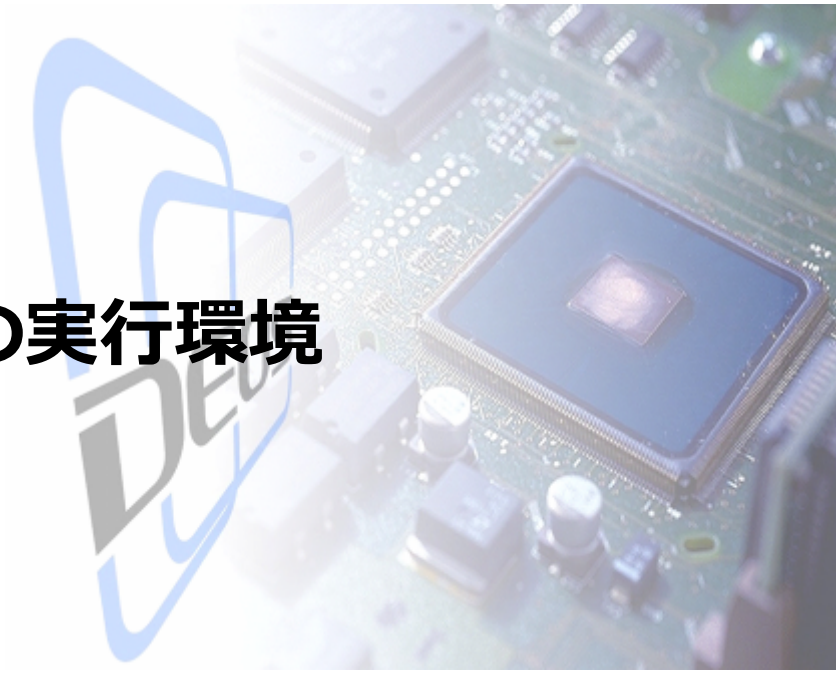

# 変化しつづける
# ディペンダブルシステムの実行環境



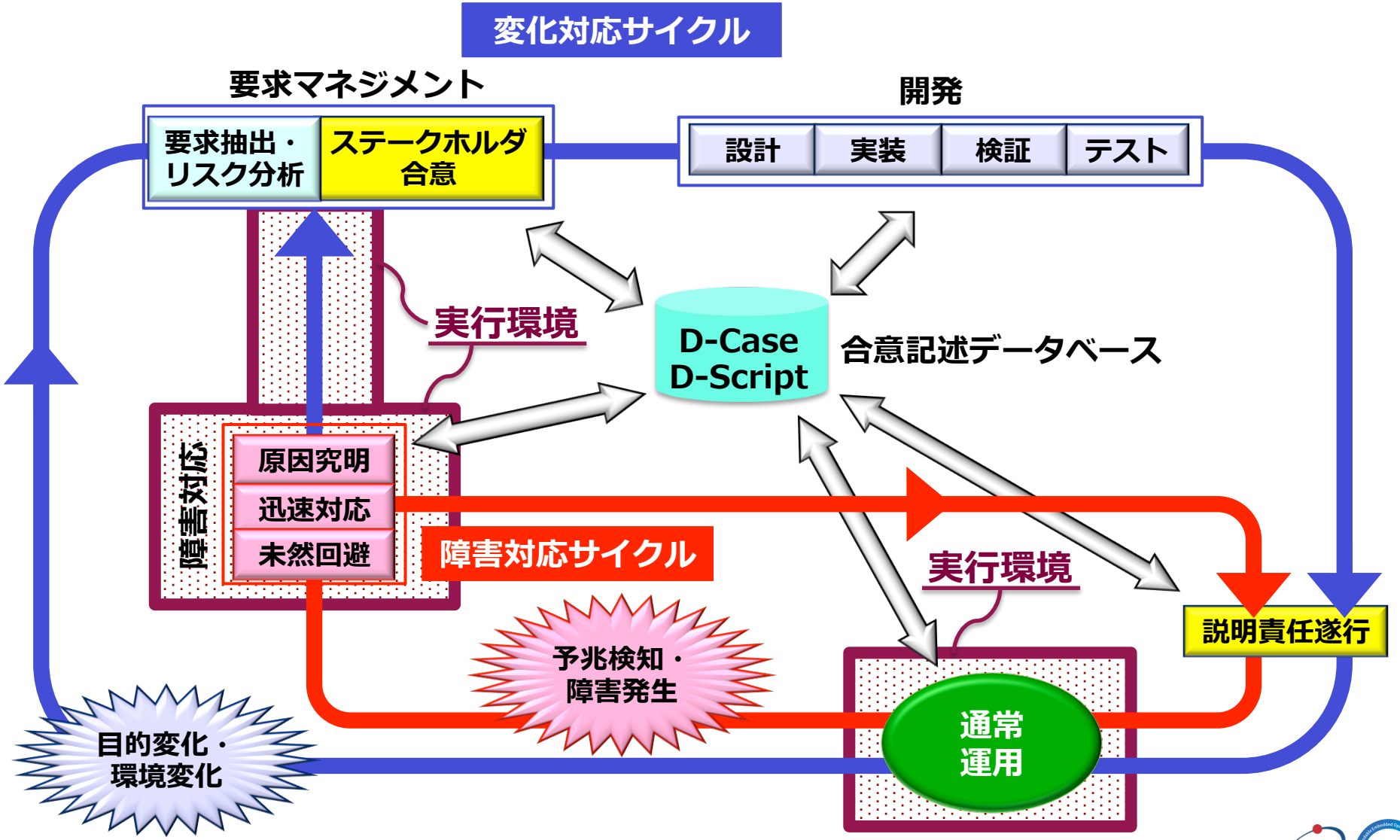
November 18, 2011

横手 靖彦
東京大学 情報基盤センター
（サイバーアイ・エンタテインメント株式会社／科学技術振興機構）

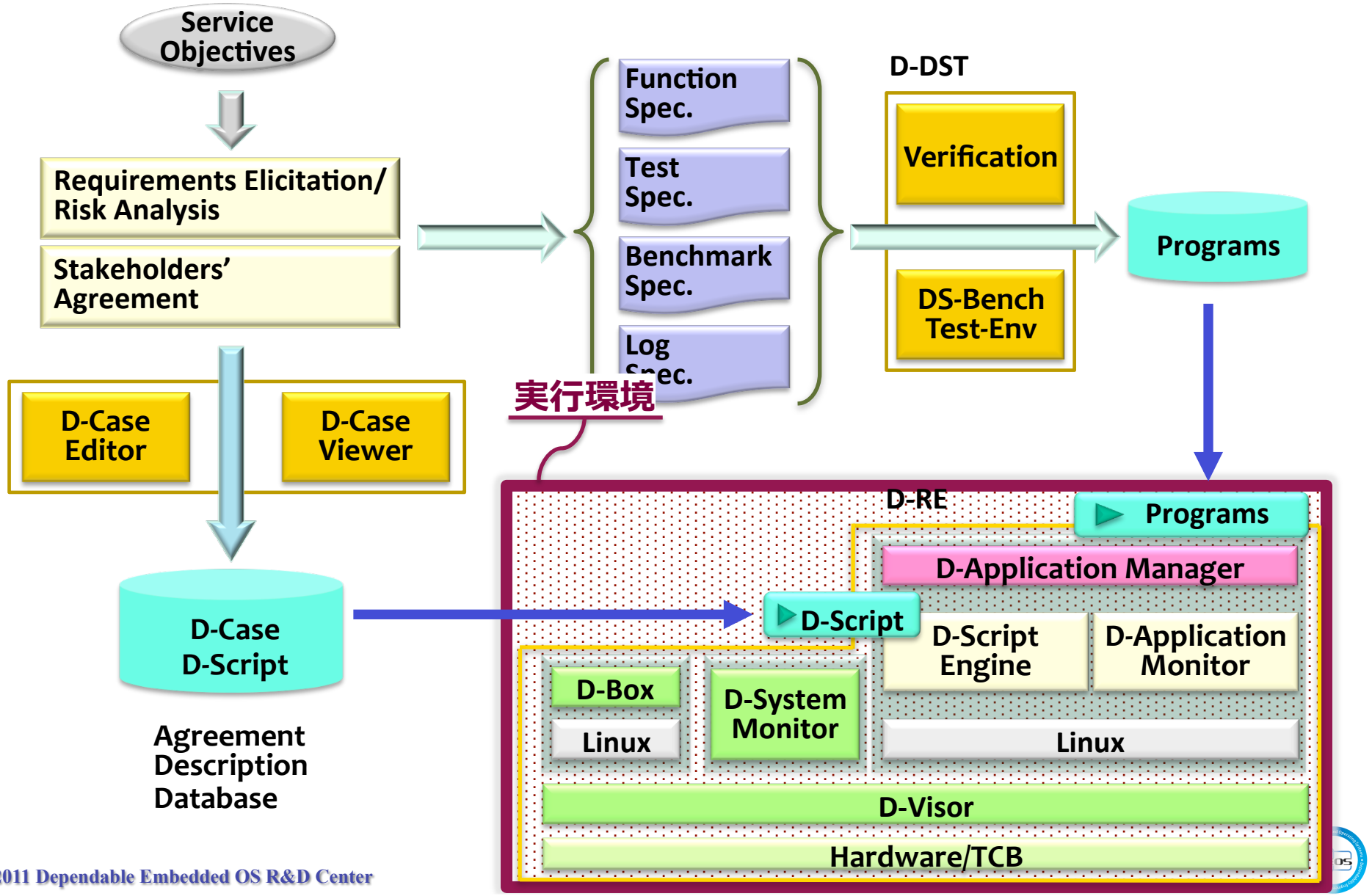
# 本日の内容

- 実行環境のDEOSプロセス／DEOSアーキテクチャにおける位置付け
- 実行環境に求められる要件
  - オープンシステムディペンダビリティを維持する為には？
  - その為の機能要求とは？
- ソフトウェア構成
  - D-＊モジュール群
- まとめ

# DEOSプロセス



# DEOSアーキテクチャ



# DEOSプロセスの運用と実行環境

- 実行環境視点からのD-Case
  - ディペンダビリティを維持するための命令セット
- D-Case視点からの実行環境
  - ステークホルダ合意に従ったディペンダビリティ維持の代理
- オンラインとオフラインの相互作用
  - D-Case記述の正確な遂行 (オンライン)
  - 実行環境状態の正確な反映 (オフライン)

D-Caseを実行環境に取り込む

オープンシステムディペンダビリティをステークホルダ合意に基づいてコントロールする。

# 実行環境 必要条件

- 付加価値
  - ディペンダビリティが担保される事がもたらすステークホルダにとっての付加価値は？
- ステークホルダの要求変更
  - 頻繁なステークホルダの要求変更に如何に迅速に対応できるか？
- 環境の変化
  - 急激な環境の変化に如何に迅速に対応できるか？

# プロセスを確実に実行する実行環境

# 実行環境への機能要求

**動作監視**

合意通りのシステム稼働を監視

**再構成**

合意された基準の逸脱からの回復

**記録**

エビデンスの記録

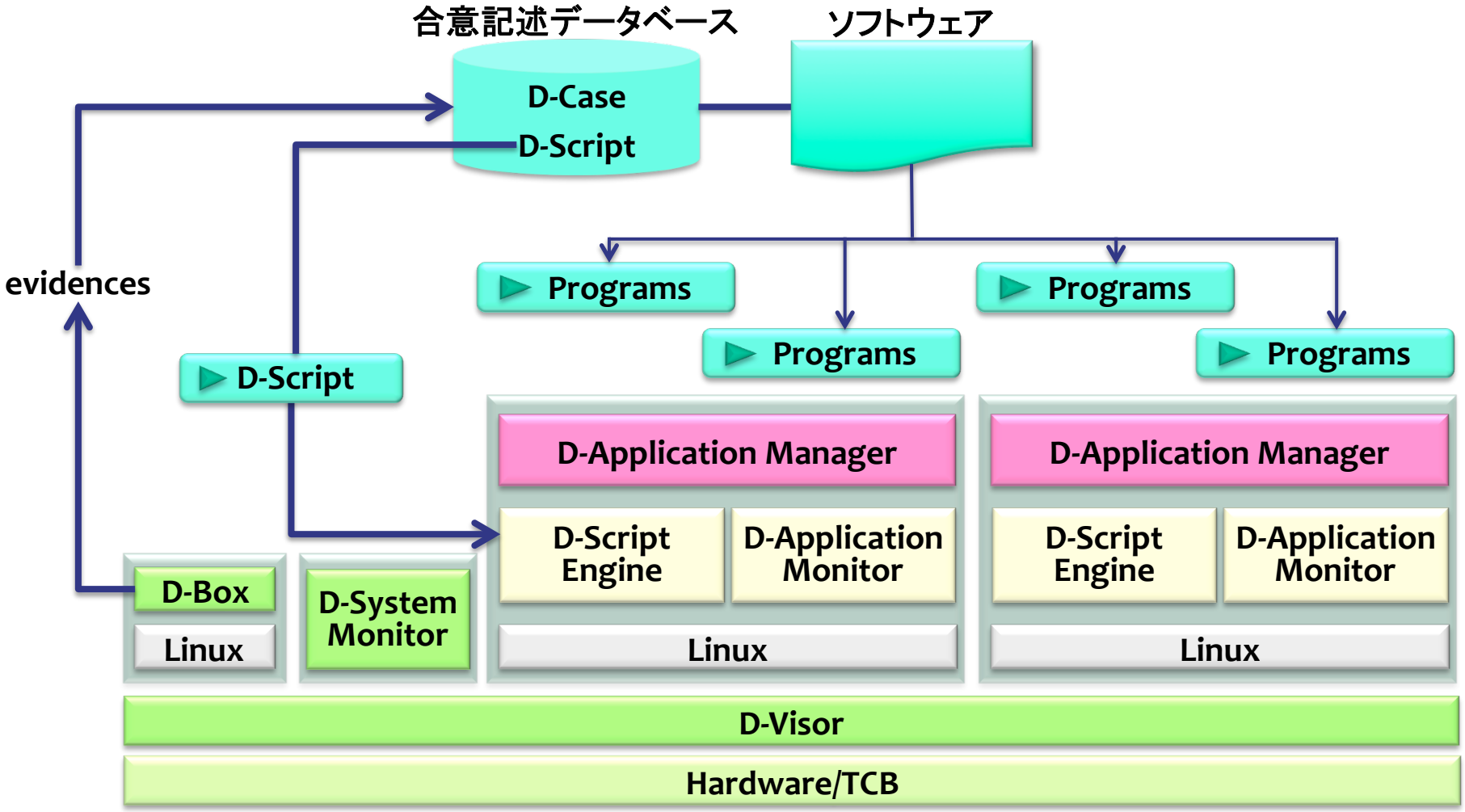
**スクリプト**

回復手順を確実・安全に実行

**セキュリティ機能**

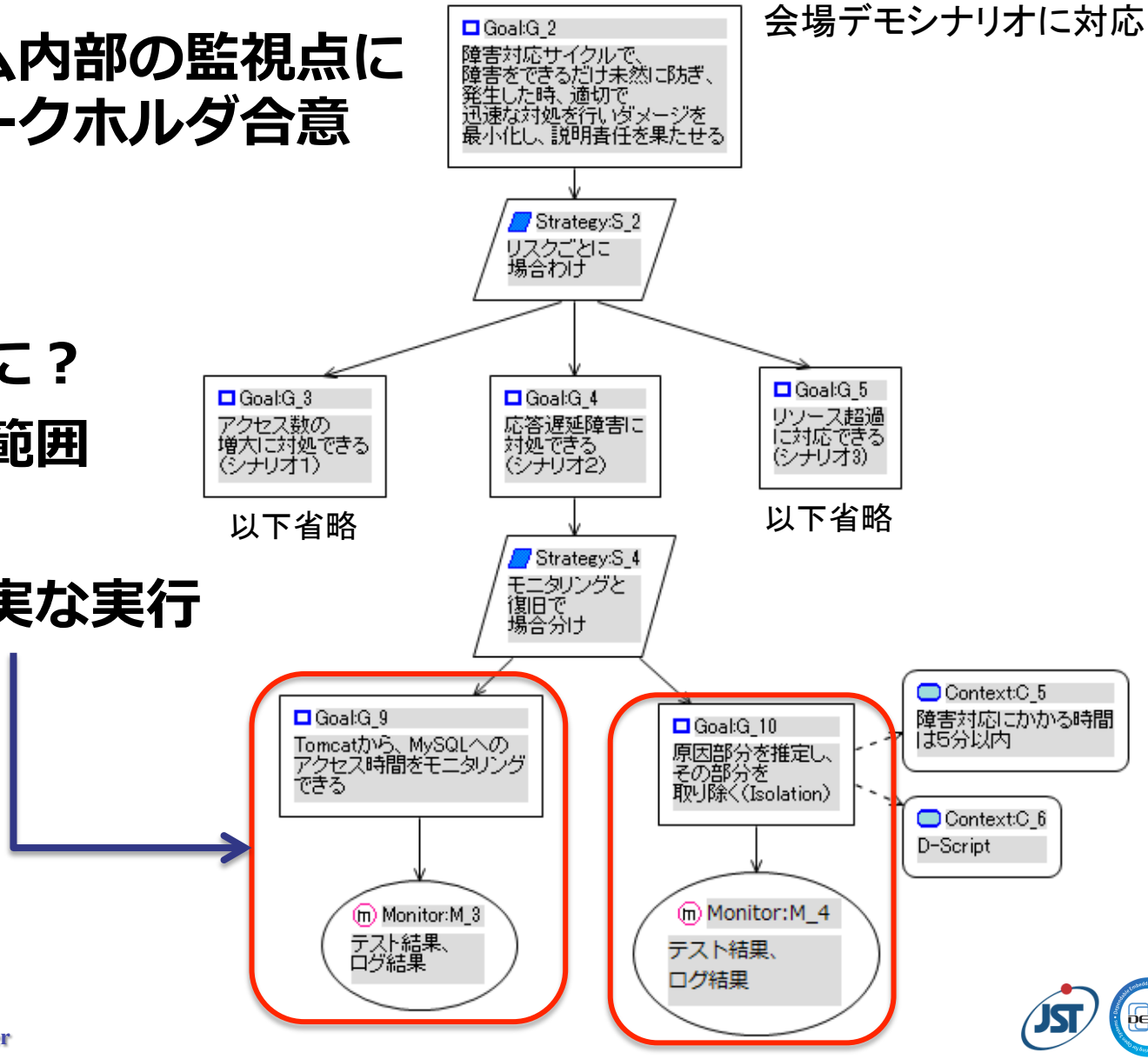
確実・安全な動作監視、再構成、スクリプト、記録の実行

# D-RE: DEOS Runtime Environment



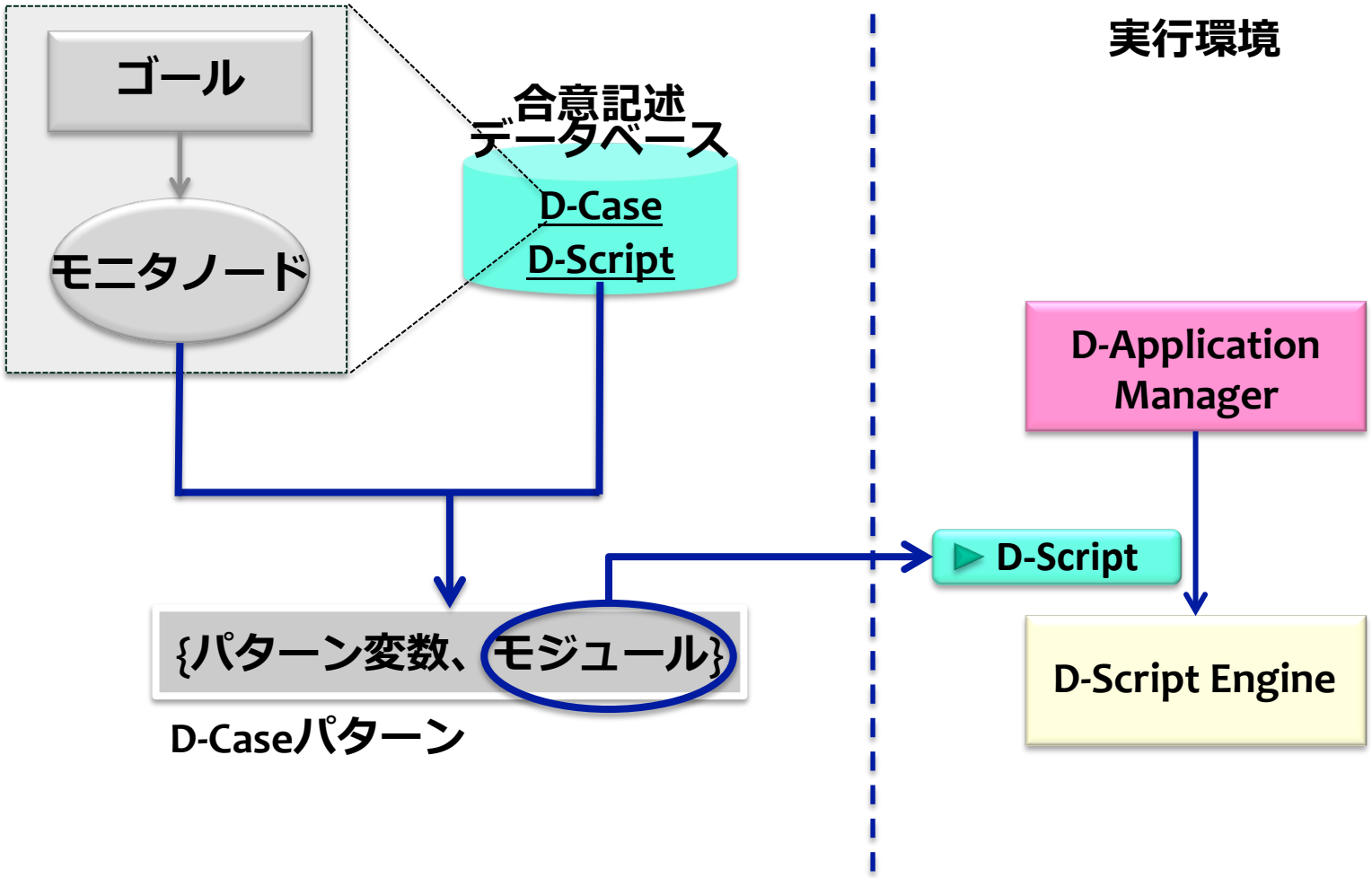
# D-Caseモニタノード

- 対象システム内部の監視点に関するステークホルダ合意
  - 何を？
  - いつ？
  - どのように？
  - 変動許容範囲
- スクリプト
  - 安全・確実な実行




会場デモシナリオに対応

# D-Case → D-Script連携



# 再構成

- Isolation
  - アプリケーション・コンテナ (Application Containers)
    - アプリケーション単位での独立性
  - システム・コンテナ (System Containers)
    - OS単位での独立性
  - 障害の影響範囲をコンテナによって制限する。

- Reconfiguration
  - コンテナ単位で再構成
  - D-Scriptによる再構成手順の実行

# D-Application Manager

- D-Awareアプリケーション
  - ディペンダビリティ維持に関して人間系と密に連携

- アプリケーションライフサイクル 状態
  - 生成
    - 実行環境に導入された状態
  - 実行中
    - 必要な動作監視が稼働し必要な記録を取得中
  - 更新中
    - 再構成中
  - 終了

# D-Box – Securing Any Information

- 確実な情報格納庫
  - １つのデバイス(部品)に１つのD-Box
  - D-Boxのチェインを構成可能
- D-Boxへのアクセスは安全・確実
  - 証明されたエンドポイント間通信
  - 暗号化された通信
- D-Boxに記録される情報には...
  - イベントやログ、およびエビデンス
  - システム構成情報
  - 暗号化の鍵
- D-Boxは一種のフライトレコーダ

# 合意記述データベース

- オープンシステム障害に対応するための知識ベース
  - 複数ステークホルダからの要求合意に向けての議論の過程とその結果を記録

- 複数ステークホルダからの要求が合意された状態
  - D-Case および D-Script を格納する。
  - 障害に関する情報も格納する。

# 構成要素

| 要素名称 | 機能概要 | 機能要求 |
|---|---|---|
| **D-Application Manager** | アプリケーションのライフサイクル管理、および複数アプリケーションの独立性を担保する仕組み(Application Containers)を提供する。 | 再構成 |
| **D-Application Monitor** | アプリケーションの動作監視機能を提供する。 | 動作監視 |
| **D-Script Engine** | D-Scriptを確実・安全に実行する。 | スクリプト |
| **D-System Monitor** | システムの動作監視機能を提供する。 | 動作監視、<br>セキュリティ機能 |
| **D-Box** | エビデンスを始め、OSD実現に有益な情報を安全・確実に記録する。 | 記録 |
| **D-Visor** | システム構成要素の独立性を担保する仕組み(System Containers)を提供する。 | 再構成、<br>セキュリティ機能 |

# まとめ

- 変化しつづけるシステムの為の実行環境
  - DEOS Runtime Environment, D-RE
  - D-Case ⇔ D-RE ⇔ D-Script
  - 持続するオープンシステムディペンダビリティ
- リファレンス実装
  - 会場にてデモ
  - Linuxパッケージとして提供
- 普及促進委員会から配布予定