

合意記述手法D-Caseと適用事例

- 合意とは
- D-Caseとは
- 医療情報システムの安全管理
- 議論分解パターン
- アーキテクチャ記述言語ArchiMate

名古屋大学 情報連携統括本部 情報戦略室
教授 山本修一郎

合意とは

意見が一致すること

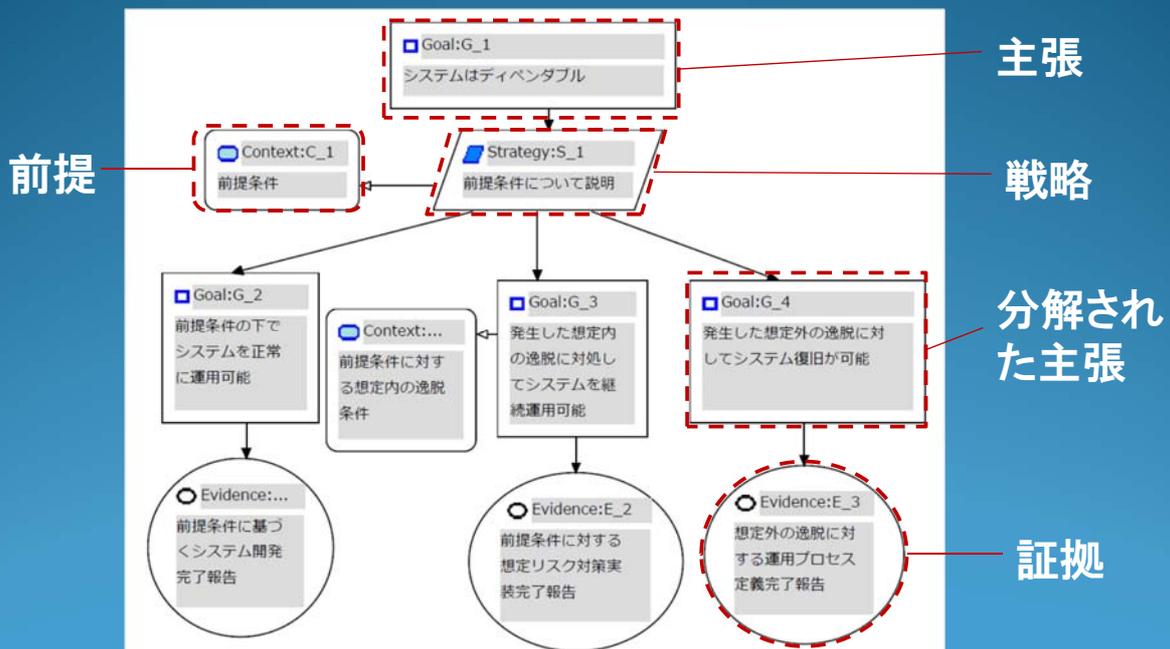
契約の成立要件: 契約当事者間の意思表示の合致

広辞苑

合意の型

- 合意条件の下で、複数の意見が一致する
 - 項目ごとに、意見が一致する
- 目標条件を対象が満たしている
 - 法律を行動が遵守している
 - 原則を行動が満たしている
- 目標条件を実現手段が満たしている
 - 要求をシステムが満たしている
 - 計画を実行結果が達成する

D-Caseとは



方法序説とD-Case

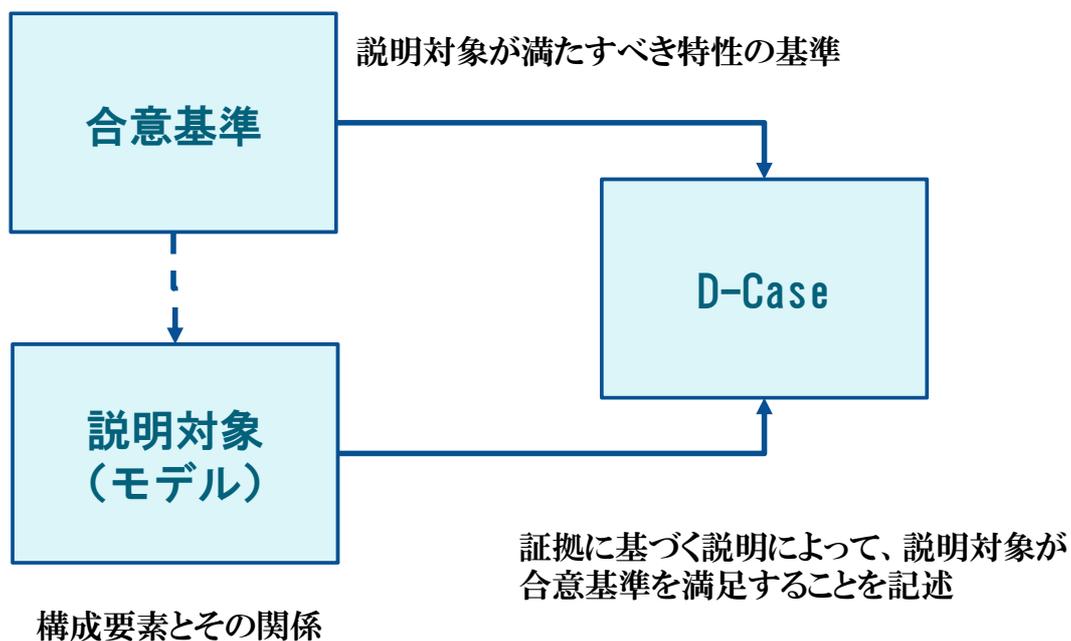
規則	方法序説	D-Case
明証性	明証的に真理であると認めるもの以外を判断の中に入れていないこと	正しさが確認された証拠であること
分析	検討しようとする難問を必要なだけの小部分に分割すること	主張を複数の下位の主張に分解すること
総合	もっとも単純でもっとも認識しやすいものから段階的にもっとも複雑なものへの認識へと昇っていくこと、	証拠によって論証できる最下位の主張から、最上位の主張を説明すること
	自然のままでは前後の順序がつかないもの間に順序を想定すること	主張を分解するための前提を明確にすること
枚挙	最後に完全な枚挙と、全体の見直しをして、見落としがないことを確信すること	最上位の主張を説明するために、完全な証拠が列挙できていること

参考)デカルト著、谷川多佳子訳、方法序説、岩波文庫、1997

Copyright Prof. Dr. Shuichiro Yamamoto 2014

5

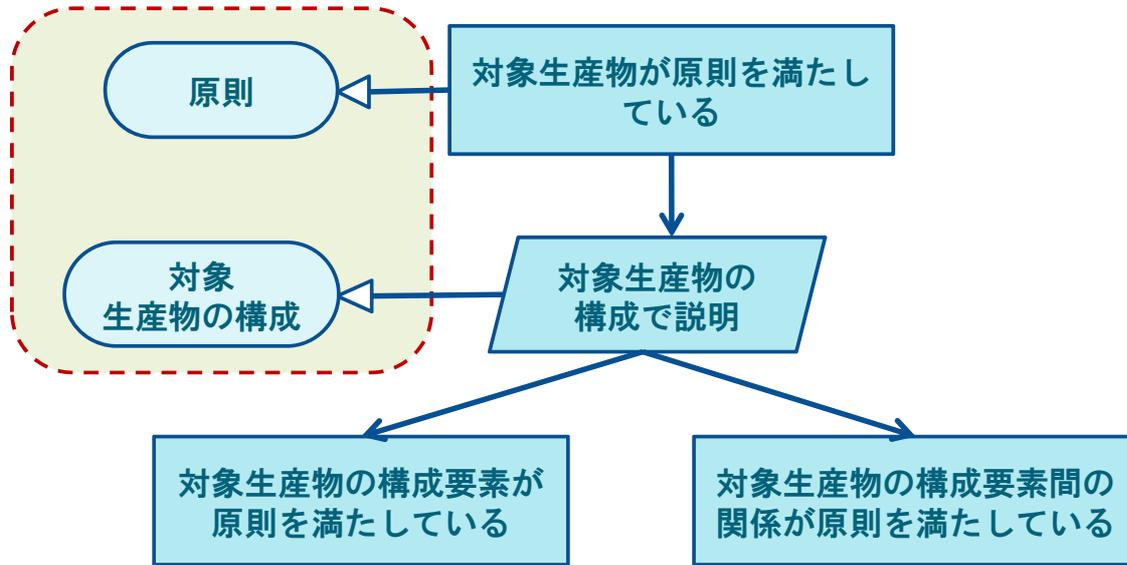
D-Caseの基本概念



Copyright Prof. Dr. Shuichiro Yamamoto 2014

6

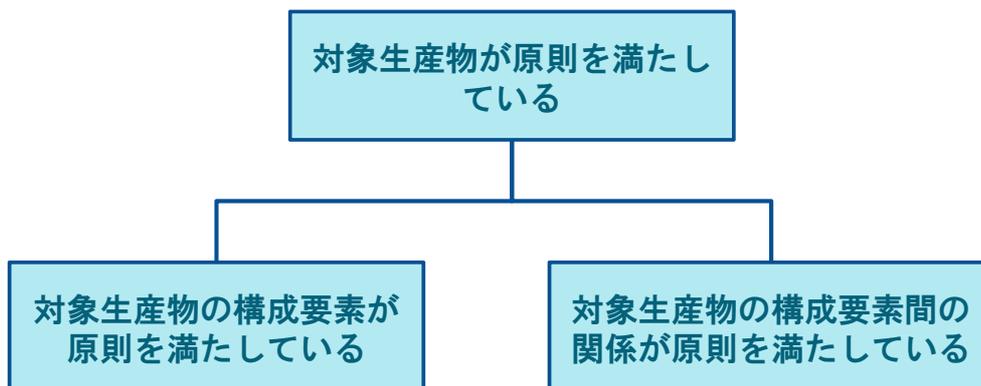
第三者への説明責任の遂行



Copyright Prof. Dr. Shuichiro Yamamoto 2014

7

論理木による第三者への説明責任の遂行



MECE (Mutually Exclusive Collectively Exhaustive)

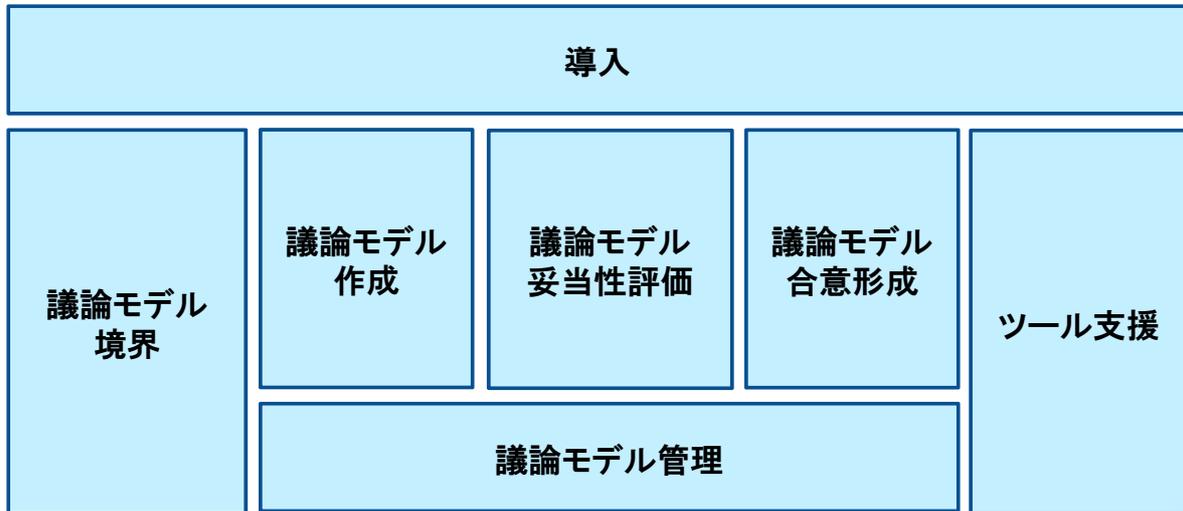
分解理由
分解の前提
証拠

論理木の図式要素では表現できない

Copyright Prof. Dr. Shuichiro Yamamoto 2014

8

D-Case シラバスの構成例



D-Case言語の設計と実装

パターン、モジュールを含む
D-Caseの言語仕様を設計、D-Case Editorで実装
→
世界ではじめてのアシュアランスケースの形式的な設計、実装



www.dsn.org

2014.6にOMGで標準化提案予定。
D-Caseが世界標準へ

本実装に基づくD-Caseパターンライブラリを公開へ

$(g, [x: = ?]) \rightarrow (g[v/x], [x: = v])$
 $(g, e, [x: = ?]) \rightarrow (g[v/x], e[v/x], [x: = v])$
 $(g, st, (P_1, \dots, P_n), [x: = ?]) \rightarrow (g[v/x], st[v/x], (P_1[v/x], \dots, P_n[v/x]), [x: = v])$
 $(g, st, c[i, j], (P_1, \dots, P_n), d) \xrightarrow{\{s_1 \dots s_k\}} (g, st, (P_{s_1}, \dots, P_{s_k}), d)$
 $(g, st, m[i, j], (P), d) \rightarrow (g, st, (P, \dots, P), d)$
(P repeats k times)
 $\mu .P \rightarrow P[\mu .P /]$
 $\mu .P \rightarrow !$

Yutaka Matsuno,
A Design and Implementation
of an Assurance Case Language
In Proc. of IEEE/IFIP DSN 2014

ディペンダビリティ分野
のトップカンファレンス
IEEE/IFIP DSN2014 (Atlanta, 6.23-26, 2014)
に採択!

44年のDSNの歴史で、日本からの採択数は10数件程度
2014年度は56本の採択論文中、
本論文のみ、日本から採択

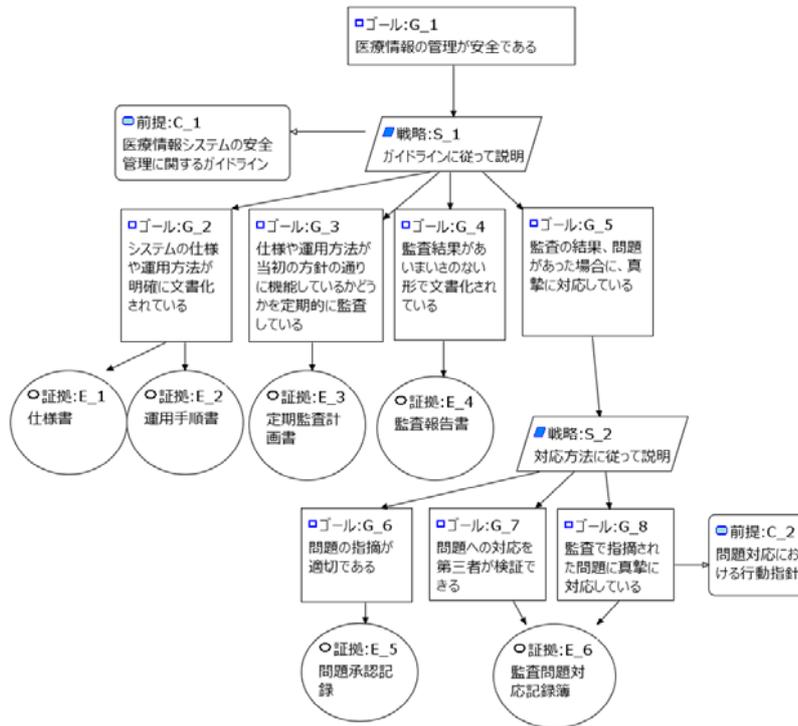
医療情報システムの安全管理

説明責任

- 電子的に医療情報を取り扱うシステムの機能や運用方法が、その取り扱いに関する基準を満たしていることを患者等に説明する責任である。
- これを果たすためには、以下のことが必要である。
 - システムの仕様や運用方法を明確に文書化すること
 - 仕様や運用方法が当初の方針の通りに機能しているかどうかを定期的に監査すること
 - 監査結果をあいまいさのない形で文書化すること
 - 監査の結果、問題があった場合は、真摯に対応すること
 - 対応の記録を文書化し、第三者が検証可能な状況にすること

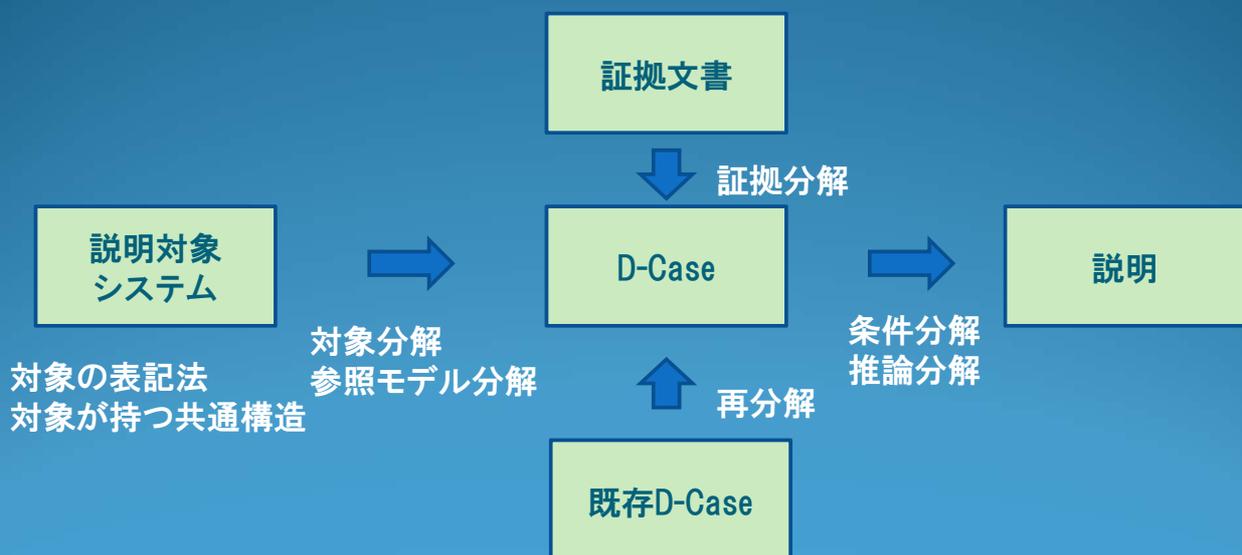
参考) 医療情報システムの安全管理に関するガイドライン、第4.1版 平成22年2月 厚生労働省
<http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf>

医療情報システム安全管理のD-Case



Copyright Prof. Dr. Shuichiro Yamamoto 2014

議論分解パターン



Copyright Prof. Dr. Shuichiro Yamamoto 2014

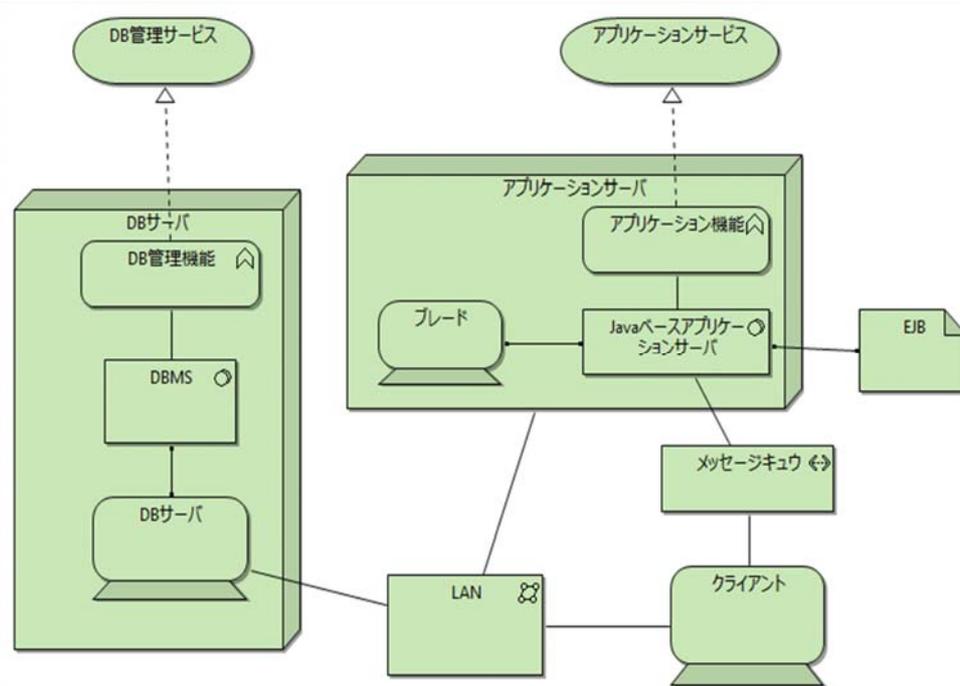
議論分解パターンの事例

分類	事例
記述法 18	アーキテクチャ, 機能, 属性, 完全化, プロセス, プロセス依存関係, 階層化, データフロー図, ビュー, ユースケース, 要求, 状態遷移, 運用要求, シーケンス図, ビジネスモデル, ゴールモデル, クラス図, 基本
参照モデル 11	DEOS プロセス, リスク, 組み込みシステム, コモンクライテリア, 要求テンプレート, システム境界, 欠陥モード, 非機能要求グレード, テストケース, 問題フレーム, アーキテクチャメタモデル
条件 8	ECA, 条件判断, 代替案選択, 矛盾解消, 平衡化, 改善, 明確化, 達成
推論 4	帰納法, 消去法, 否定推論, 反駁
証拠 11	法制度, 形式的証明, モデル検査, 試験成績書, 合意文書, レビュー報告書, シミュレーション, 評価報告書, 説明書, モニタノード, 文書
再利用 2	水平分解, 垂直分解

ArchiMateへの適用事例

分類	TOGAFアーキテクチャ開発フェーズ
ArchiMate コア	ビジネス・アーキテクチャ 情報システム・アーキテクチャ 技術アーキテクチャ
動機づけ拡張	準備 アーキテクチャ・ビジョン アーキテクチャ変更管理 要求管理
実装・移行拡張	機会とソリューション 移行計画 実装・ガバナンス

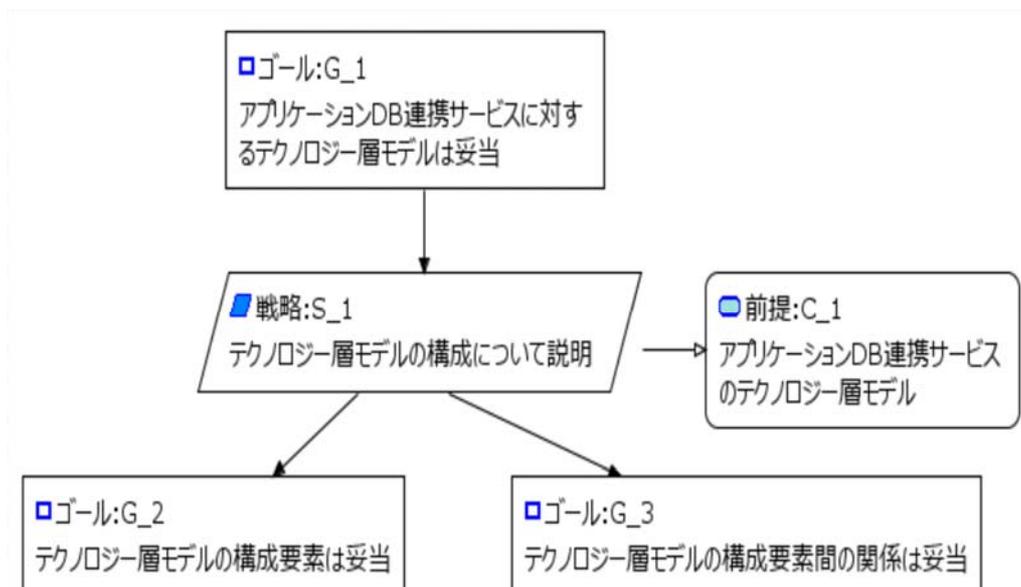
アプリケーションDB連携サービスに対するテクノロジー層モデルの例



Copyright Prof. Dr. Shuichiro Yamamoto 2014

17

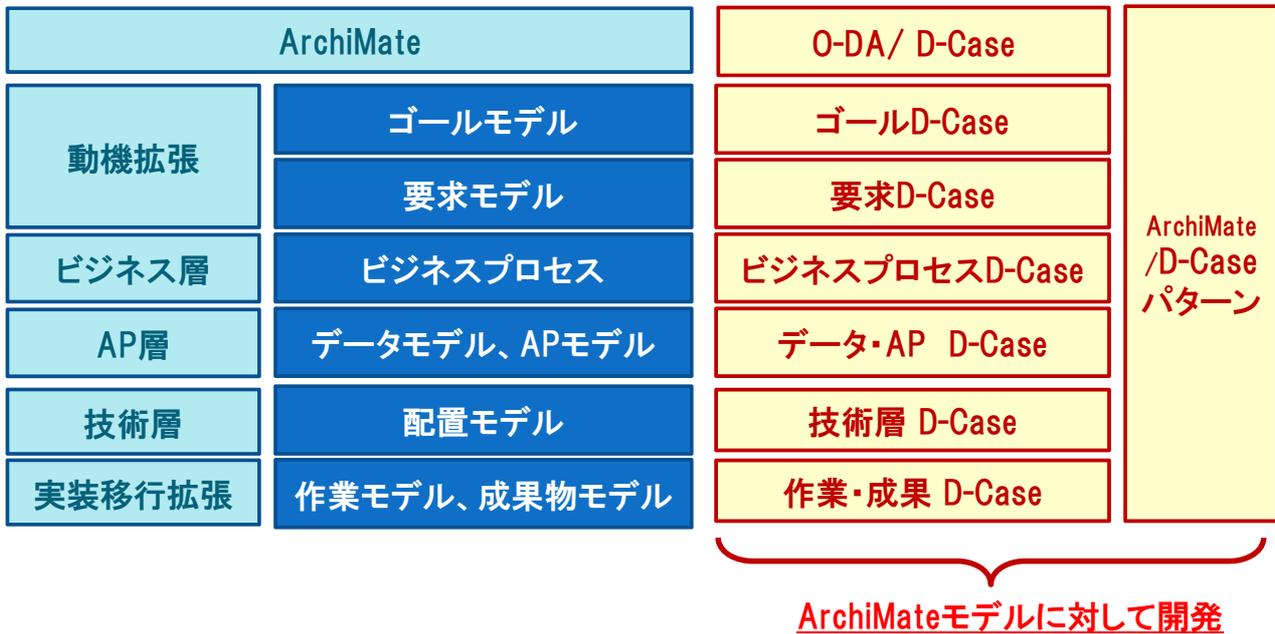
テクノロジー層モデル例の保証ケース(全体)



Copyright Prof. Dr. Shuichiro Yamamoto 2014

18

ArchiMateのためのD-Case方法論



まとめ

- 合意記述
- D-Caseの基本概念
- 医療情報システムの安全管理
- 議論分解パターンの適用事例
- アーキテクチャ記述言語ArchiMateへの適用事例