要求の品格：現実世界とシステム世界とを繋ぐ

2007/01/31

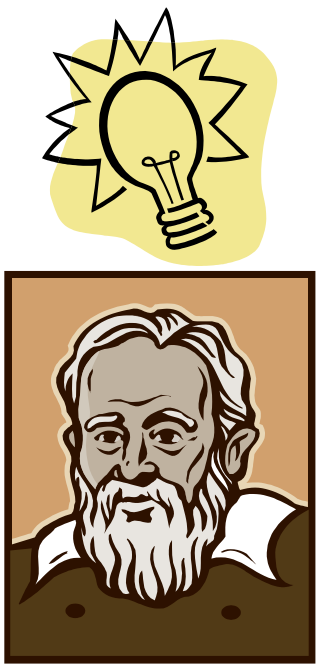
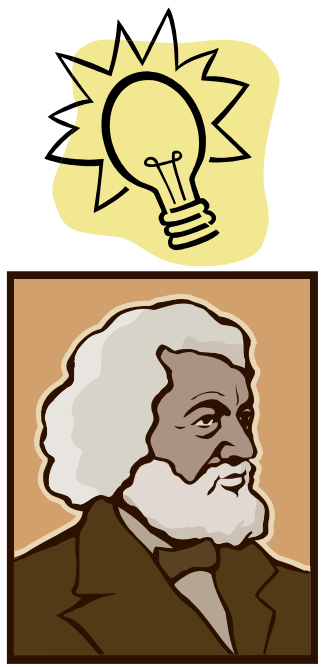
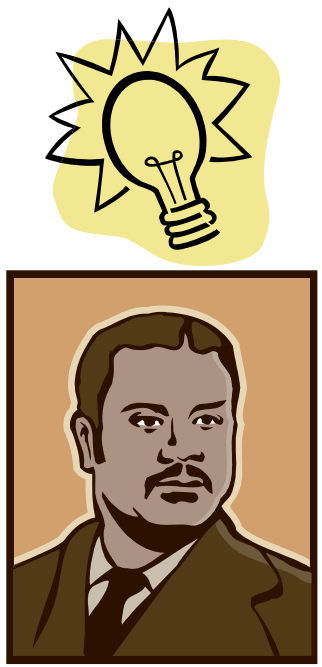
㈲ エス・ラグーン
中谷 多哉子

目次

- 要求とは
- 要求の質を高めるために
- 要求仕様書の品質
- 機能要求と非機能要求
- Misuse Caseと問題フレーム
- ESIM法
  - 正常系要求と非正常系要求
- 要求獲得とテスト

要求とは

- 要求とは，要求者の頭の中に存在する
  - 個人的な錯覚とかもしれない．

「もの」と「こと」

- 要求者から得られる「要求」は，要求者自身しか説明できないもの．
  - 要求獲得で，「もの：1次元」を「こと：多次元」として説明できれば，より多くの人々が理解できる「もの」になる
- 列挙された要求＝1次元
- シナリオ，UML，DFD.....
  - →多次元，多視点も可

要求を「こと」として表す

- たとえば，要求を，問題と，解決手段としての要求との関係によって表す
  - 事前：本当に問題解決手段はそれだけか？
  - 事後：それで問題は解決できたか？
- たとえば，業務というプロセスと，それを支援する要求との関係を用いて，「要求」を表す
- たとえば，情報資源と，それを取り扱うための要求との関係を用いて「要求」を表す．．．などなど

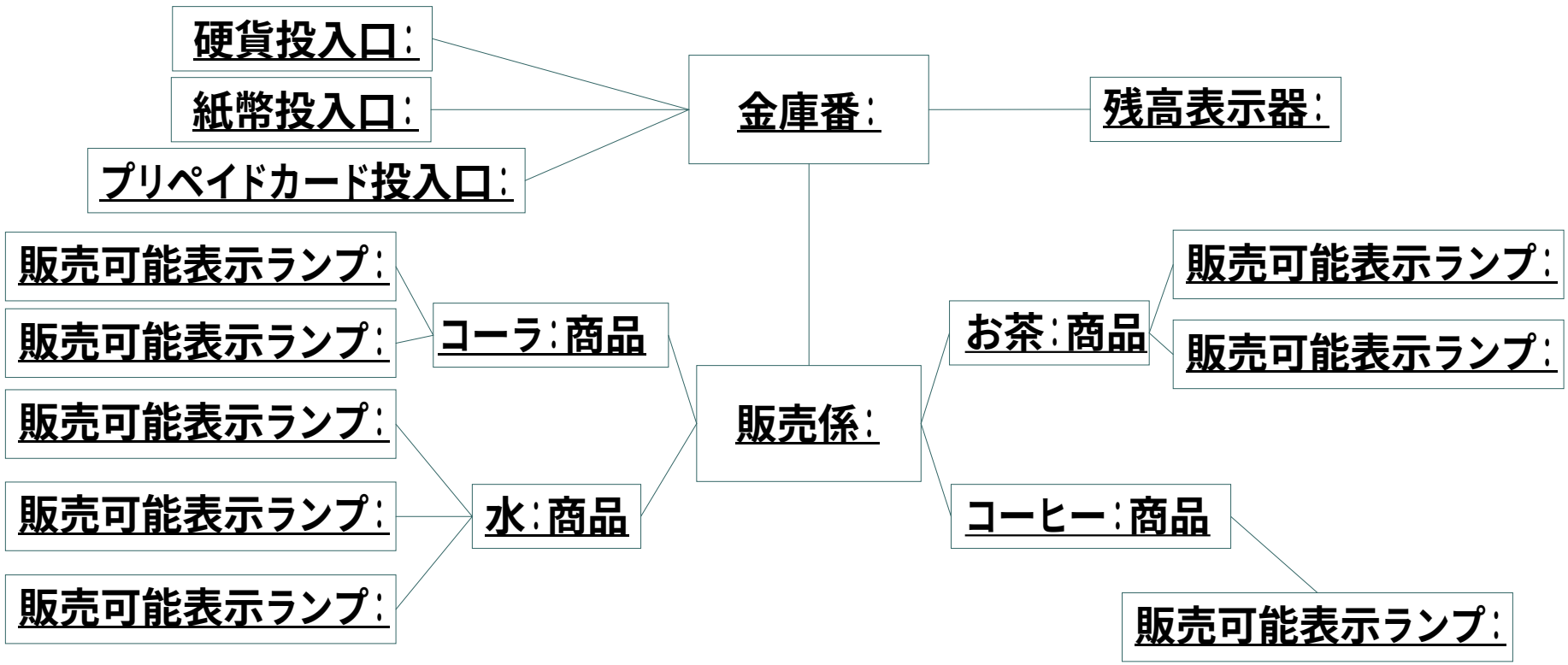
ユースケース記述：自動販売機の例

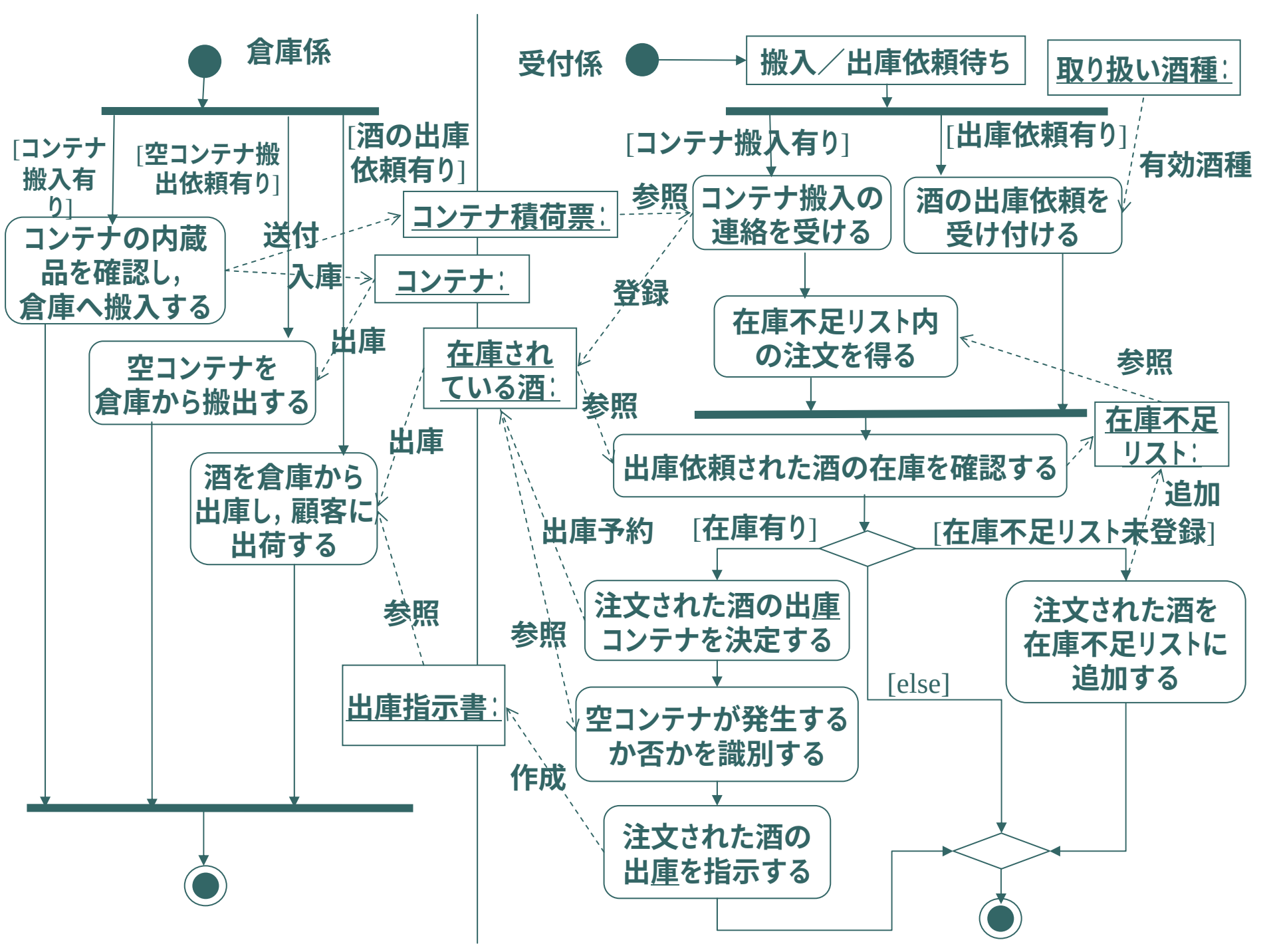
- ユースケース名：代金投入
- アクター：代金投入する購入者
- 目的：投入された貨幣の額に応じて，販売可能な商品が購入可能であることをアクターに知らせる．こと
- レベル：主レベル（利用者から直接呼ばれる）、必須、詳細
- 事前条件：代金投入が可能である
- 基本系列：
  1. アクターは貨幣をシステムに渡す．
  2. システムは，読み飛ばすことなく投入された貨幣の正当・不当判定を行う．
  3. システムは正当な貨幣だけを受付け，投入された貨幣の合計金額を求めて，アクターに通知する．
  4. システムは，投入された額に応じて販売可能な商品をアクターに知らせる．
- 事後条件：投入された貨幣の合計金額と金額に応じて購入可能な商品がアクターに知らされている．

以下省略

オブジェクト図の例

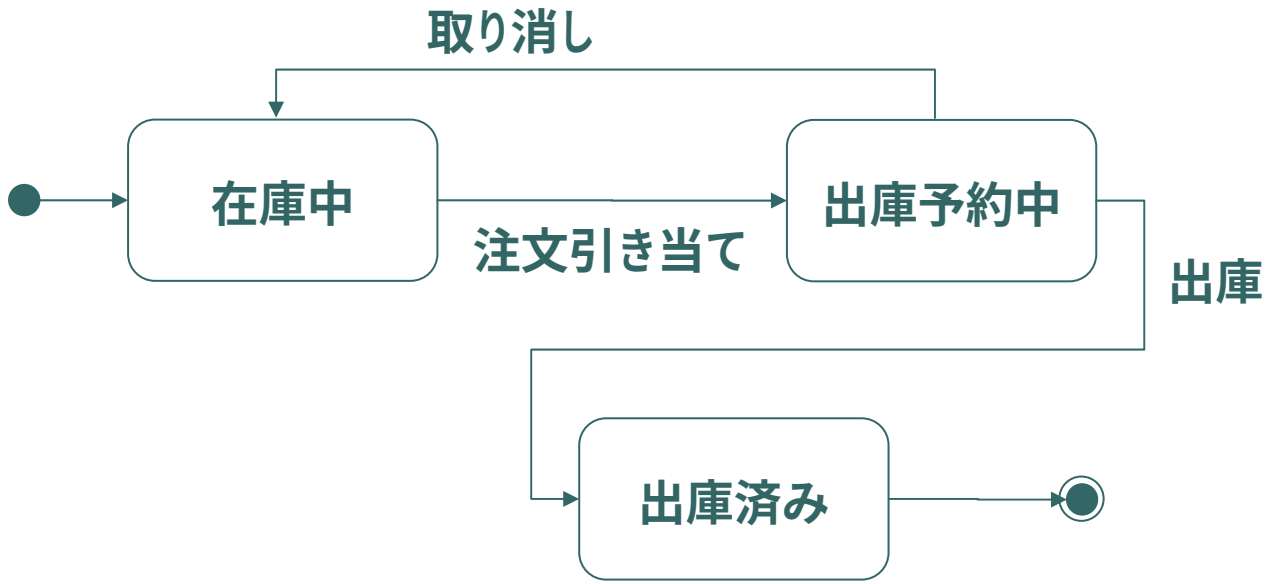
- 代金投入から販売可能表示ランプ点灯まで



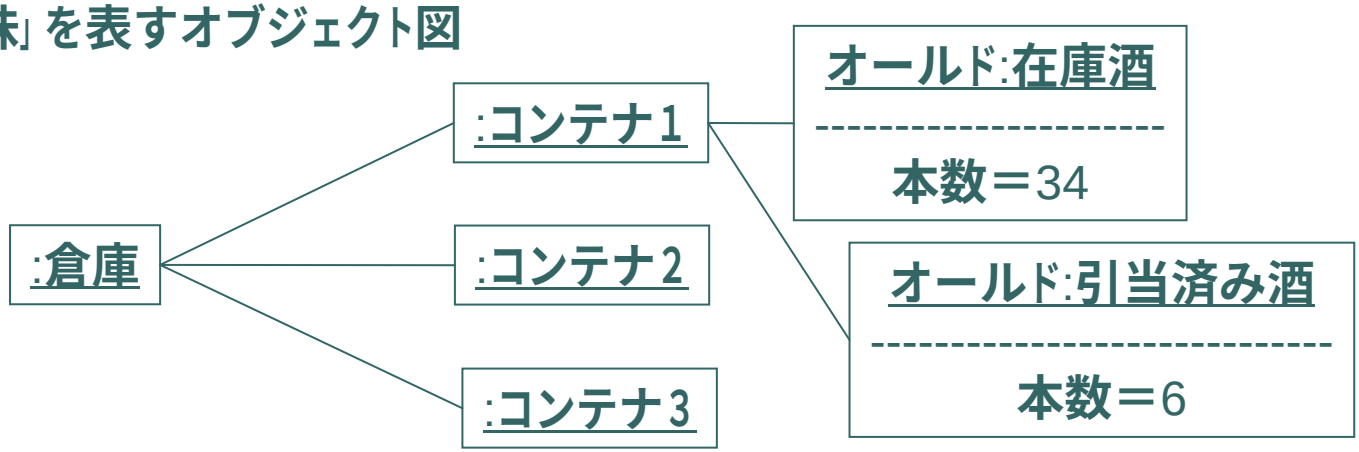

倉庫係
[コンテナ搬入有り]
[空コンテナ搬出依頼有り]
[酒の出庫依頼有り]
コンテナの内蔵品を確認し，倉庫へ搬入する
送付
入庫
コンテナ積荷票：
コンテナ：
出庫
空コンテナを倉庫から搬出する
在庫されている酒：
出庫
酒を倉庫から出庫し，顧客に出荷する
参照
出庫指示書：
作成
受付係
搬入／出庫依頼待ち
取り扱い酒種：
有効酒種
[コンテナ搬入有り]
[出庫依頼有り]
参照
コンテナ搬入の連絡を受ける
酒の出庫依頼を受け付ける
登録
在庫不足リスト内の注文を得る
参照
在庫不足リスト：
参照
出庫依頼された酒の在庫を確認する
追加
出庫予約
[在庫有り]
[在庫不足リスト未登録]
[else]
注文された酒の出庫コンテナを決定する
注文された酒を在庫不足リストに追加する
参照
空コンテナが発生するか否かを識別する
注文された酒の出庫を指示する

坂や倉庫問題における酒の状態遷移とオブジェクト抽出

酒の状態遷移図



倉庫の「意味」を表すオブジェクト図



要求の質を高めるために

- 根拠を示すこと
  - 問題と手段（＝要求）の関係を明らかにするという意味
  - 要求を満たすことがシステム開発の目的ではない．
  - 目的は，要求が発せられた根拠に対する解を与えること．
    - →解となったか否かをテストしなければならない
- 満たした／満たしていないを評価可能なように定義すること
  - 非曖昧性，検証可能性を高める

ユースケース記述：自動販売機の例（再掲）

これは目的を明記したユースケース記述

- ユースケース名：代金投入
- アクター：代金投入する購入者
- 目的：投入された貨幣の額に応じて，販売可能な商品が購入可能であることをアクターに知らせる．こと
- レベル：主レベル（利用者から直接呼ばれる）、必須、詳細
- 事前条件：代金投入が可能である
- 基本系列：
  1. アクターは貨幣をシステムに渡す．
  2. システムは，読み飛ばすことなく投入された貨幣の正当・不当判定を行う．
  3. システムは正当な貨幣だけを受付け，投入された貨幣の合計金額を求めて，アクターに通知する．
  4. システムは，投入された額に応じて販売可能な商品をアクターに知らせる．
- 事後条件：投入された貨幣の合計金額と金額に応じて購入可能な商品がアクターに知らされている．

以下省略

手段が確定したユースケース記述の例

1. アクターは紙幣投入口，硬貨投入口，プリペードカード読み取り機に手で貨幣を投入し，システムに渡す．
2. システムは，代金投入を中断し，投入された貨幣の正当・不当判定を行う．
3. システムは正当な貨幣だけを受付け，投入された額に対して，新たに投入された貨幣の金額を足し，合計金額を求める．
4. システムは求めた金額を残高表示器に表示してアクターに通知する．
5. システムは，投入された額に応じて販売可能な商品の販売ランプを点灯して，販売可能な商品をアクターに知らせる．
6. ・・・・・

以下省略

要求仕様書の品質 (IEEEstd.830-1998)

- 正当性：記述が正しいか，妥当か
- 非曖昧性：二通り以上の解釈が成り立たないか
- 完全性：すべての項目が記述されているか
- 一貫性：矛盾がないか
- ランク付け：変わりやすさ，重要性に関して優先順位（必須，条件付き，選択的付加価値）が示されているか
- **検証可能性：要求を満たしたか否かを検証可能な記述**
- 変更可能性：記述に重複がないか，参照先は明示されているか，参照されやすいか（＝ラベル付け）．
- 追跡可能性：前向き追跡可能性，後ろ向き追跡可能性

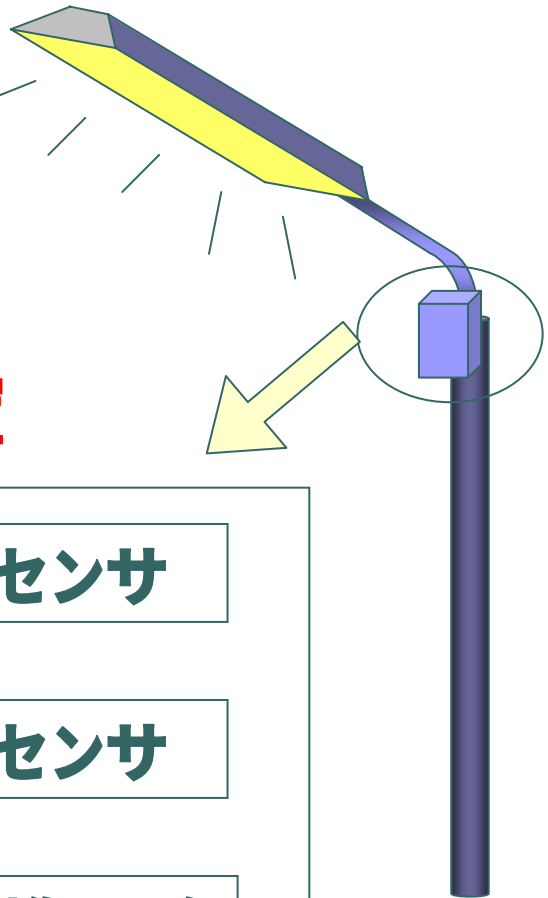
機能要求と非機能要求

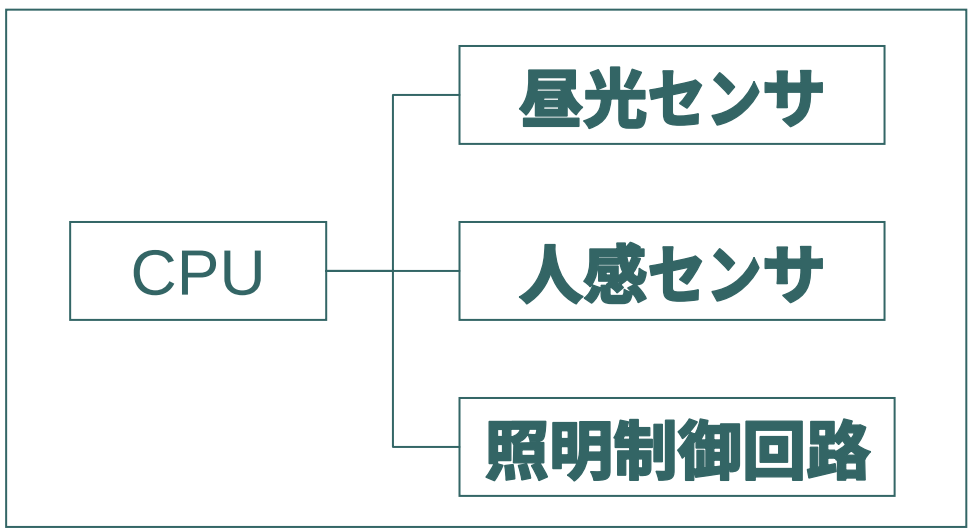
- 機能要求：システムが特定の目的を達成するために持つべき機能の要求
  - 「できる」か「できない」かを基準として，テスト可能
- 非機能要求：機能要求が（目的達成のために）持つべき性質，性能
  - テストのために定量的に定義

→達成できていることを検証可能となる

道路灯の要求定義

- 機能要求：夜間に人が近づくと点灯する
- 非機能要求：省エネを満足しながら，通行人の安全性を確保する．





安全性とは？

- . . . という使い方に対して障害を起こさない. (目的)
  - . . . という使い方に対して, システムは. . . と動作する. (手段)
- システムが. . . という故障を発生したとき, . . . とならない (目的)
  - . . . とシステムは動作する.
- ✗ 飛ばない飛行機, 走らない車は (システムとして) 安全だが, システムに期待される現実世界の目的は達成できない.

システムと現実世界とを観察し, 関連づける技術が必要

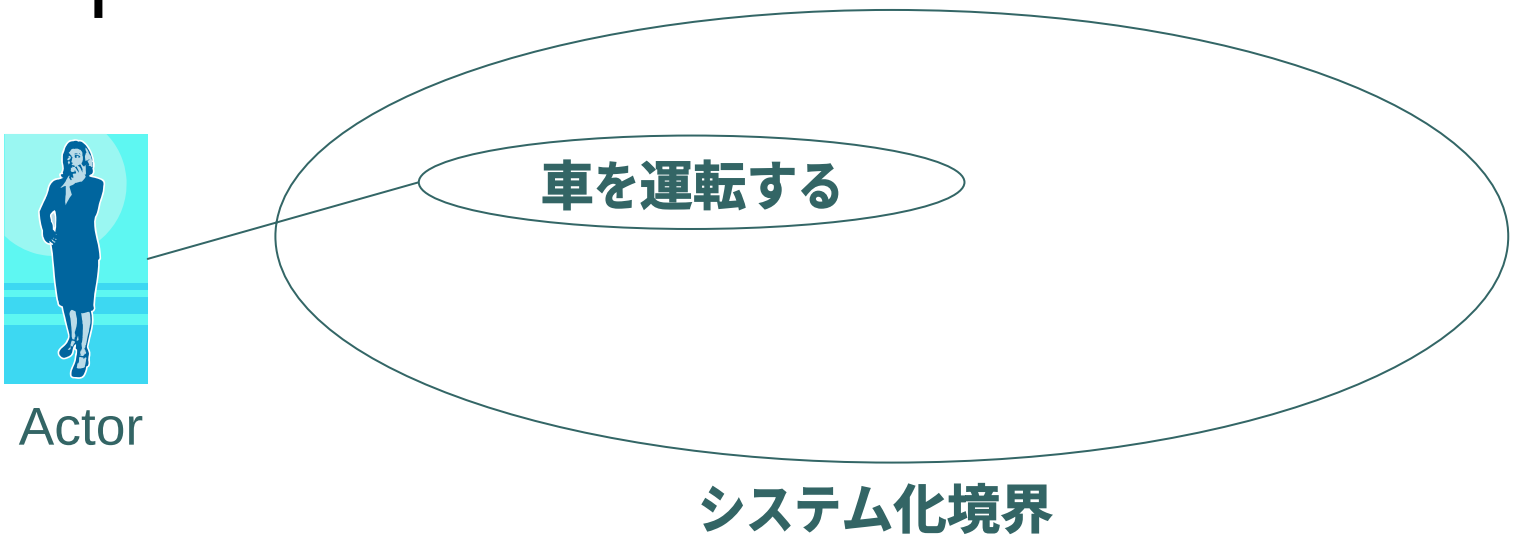
MisuseCaseと問題フレーム

システムと現実世界とを繋ぐ技術

Misuse Case

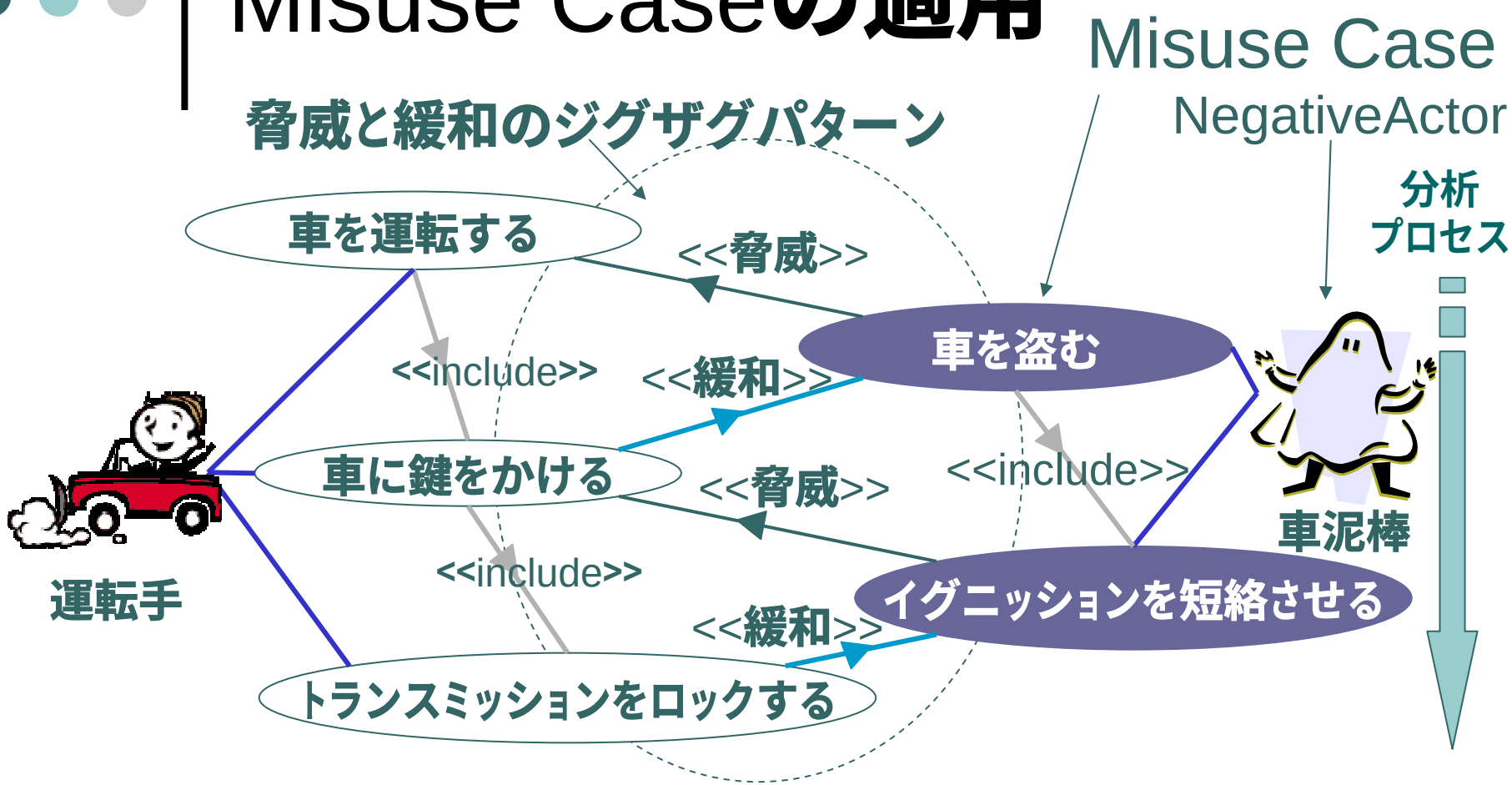
- Misuse caseとは
  - 設計中のシステムに対する敵対的なアクターの視点から記述するユースケース
- ユースケースとミスユースケースを設計中のシステムのシナリオのモデル化や分析に使うことで，脅威を軽減し，機密性を向上させることができる．
- ミスユースケース (MuC)の中には，非常に稀な状況で発生するものもあるし，継続的にシステムの脅威となるものもある．
  - 駐車中の車には盗難の脅威
  - Webサーバには DoS攻撃の脅威

通常のUse Case図



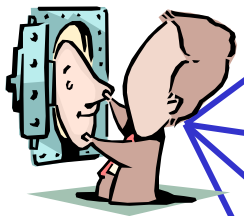
- これで安全なシステムを構築することができるか
- 要求は抜けていないか．目的は達成できるか．
- 目的達成に対する脅威はないか．あるとしたら，それに対する対処は？

Misuse Caseの適用



- 「車を運転する」ことで「車を盗む」という脅威にさらされる．
- 「(脅威軽減のための派生要求) 車に鍵をかける」ことは「車を盗む」という脅威を緩和させる．
- 「車に鍵をかける」ことは「イグニッションを短絡させる」という脅威にさらされる．
- 「トランスミッションをロックする」ことで，「イグニッションを短絡させる」という脅威を緩和させる．

金庫のMisuse Caseの例



宿泊客

貴重品を預ける

金庫に施錠する

金庫を解錠する

金庫の貴重品を取り出す

重い金庫を使用する

頑丈な金庫を使用する

秘密鍵を使用して
金庫を解錠する

解錠者の認証検査を行い
解錠履歴を残す

ホテル
支配人

<<脅威>>

<<緩和>>

貴重品を盗む

金庫ごと盗む

金庫を壊す

秘密鍵を盗む

鍵を忘れる

鍵をかけたままチェックアウトする

泥棒

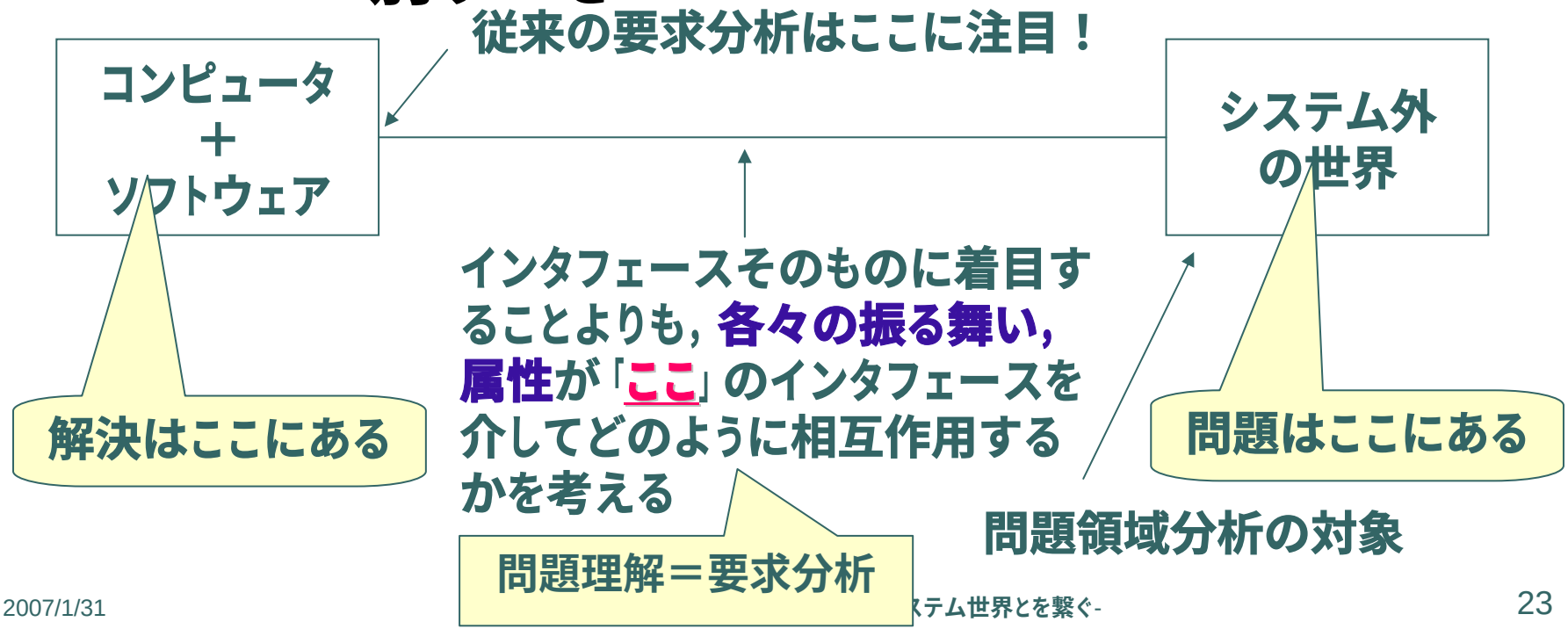
忘れっぽい
宿泊客

問題フレーム：問題の所在を明らかにし，分析する関心対象を絞り込む枠組み

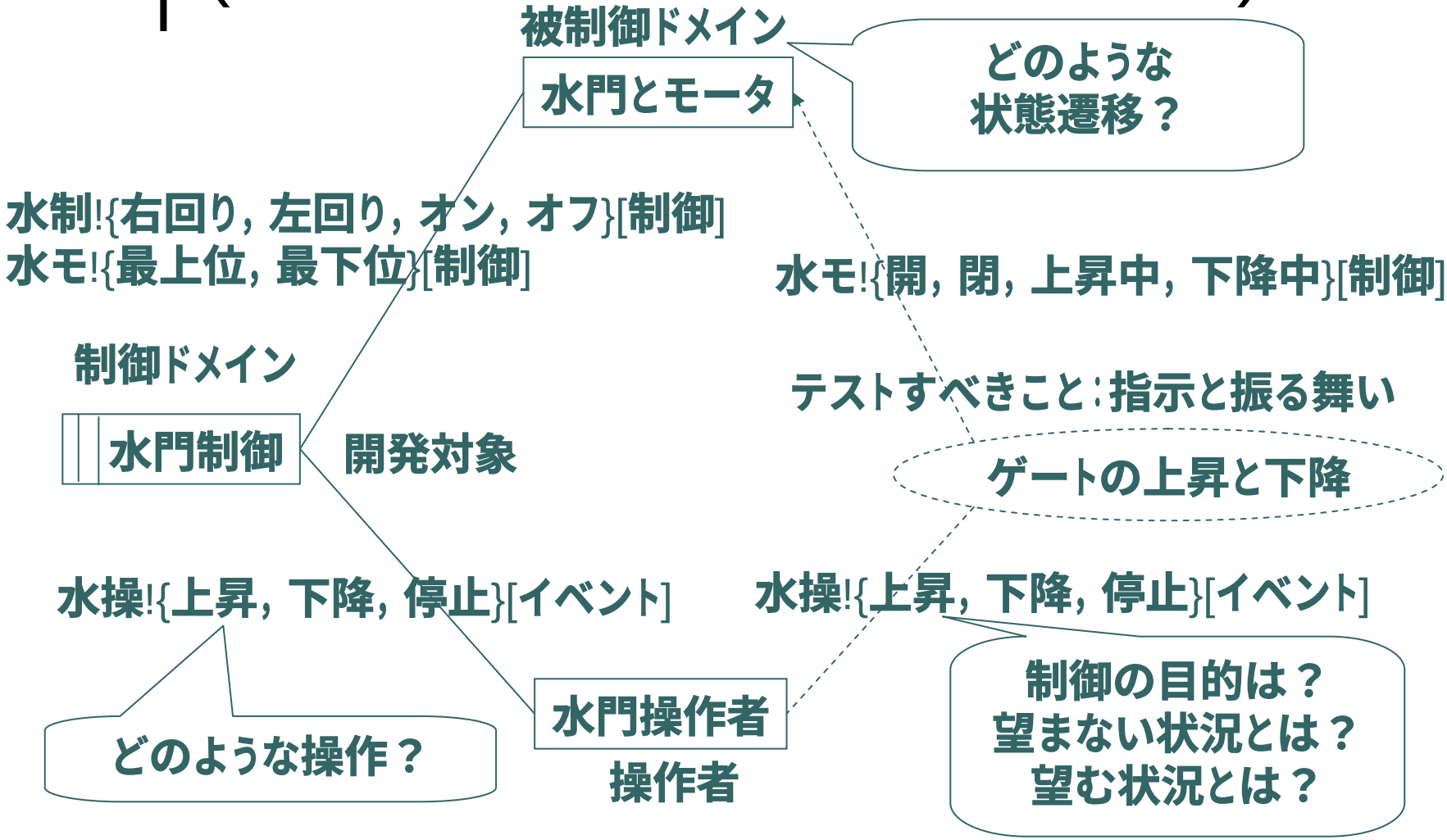
Michael Jackson: **Problem Frames, Addison-Wesley, 2001.**

問題フレームが示唆する新しい視点

- 問題解決よりも問題の識別が重要
  - WhatとHowの識別よりも「Where」で識別すべき



水門問題の例
(Commanded Behaviorフレーム)



問題フレームから得られる知見

- 要求分析を行うには，開発対象だけを観察するだけでは不十分
- 開発対象を取り巻く環境を分析することによって，相互作用，因果関係を明示することができる
  - 開発対象の外部環境で発生する例外，異常，正常の各シナリオを抽出するために必須

MisuseCaseと問題フレーム

- **意図：システムへの要求と現実世界との繋ぎ部分から要求を獲得する**
- **テストへの期待：**
  - **システムが意味を持つことを確認してもらいたい→正しさ（検証**Verification）**だけでなく，意味を持つこと（妥当性確認**Validation）

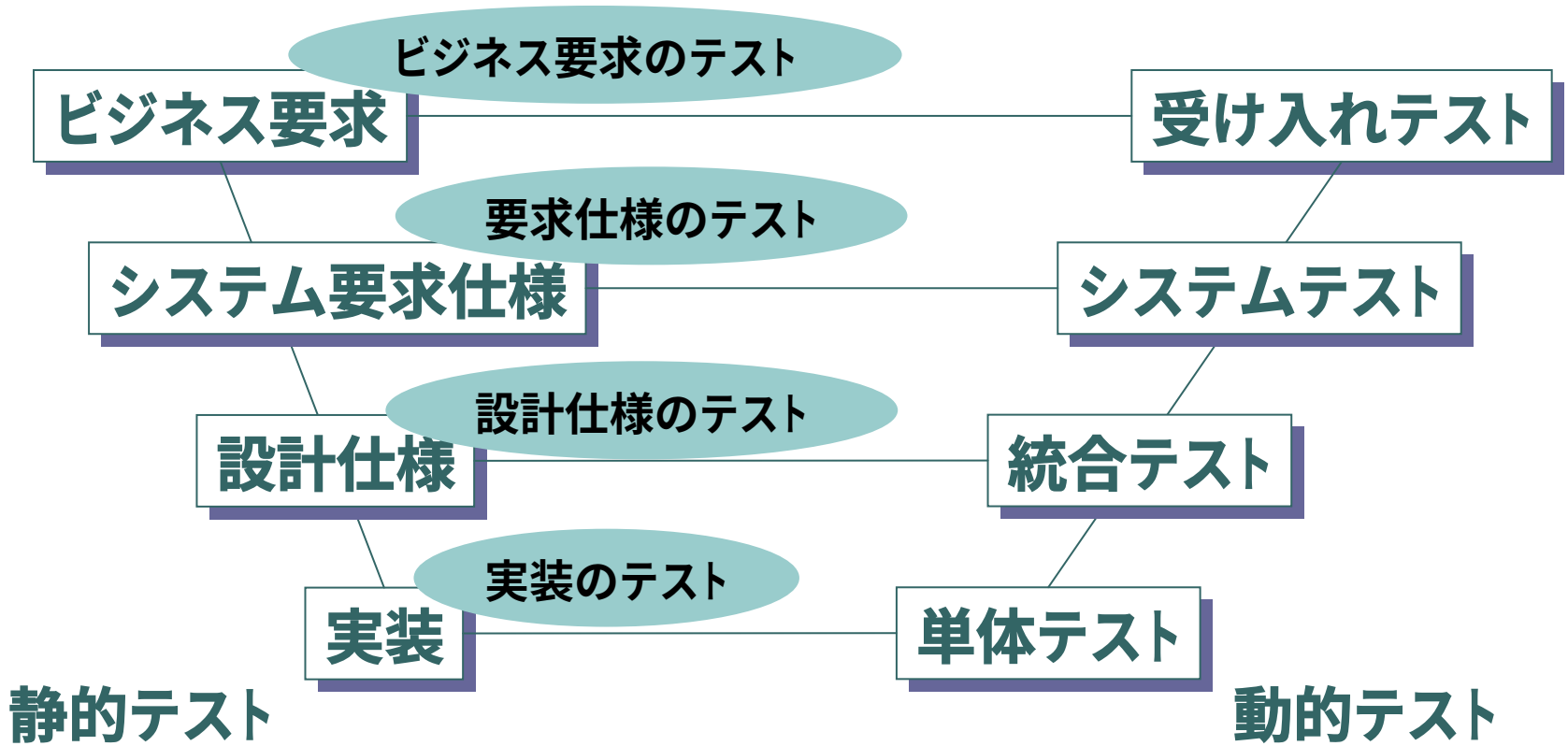
要求獲得とテスト

“Testing to improve requirements”, Dorothy Graham, Grove Consultants, (09/14,RE’06).

テスト可能な要求を仕様化するために

- 要求が先かテストが先か
  - テストできる要求を定義する！これが要求仕様の品質改善の早道
  - テストの実行は成果物に対して，テストケースの設計は要求に対して→要求の改善へ
  - 要求獲得プロセスにテスト担当者の同席は必須

要求プロセスとテストプロセスとの融合に向けて



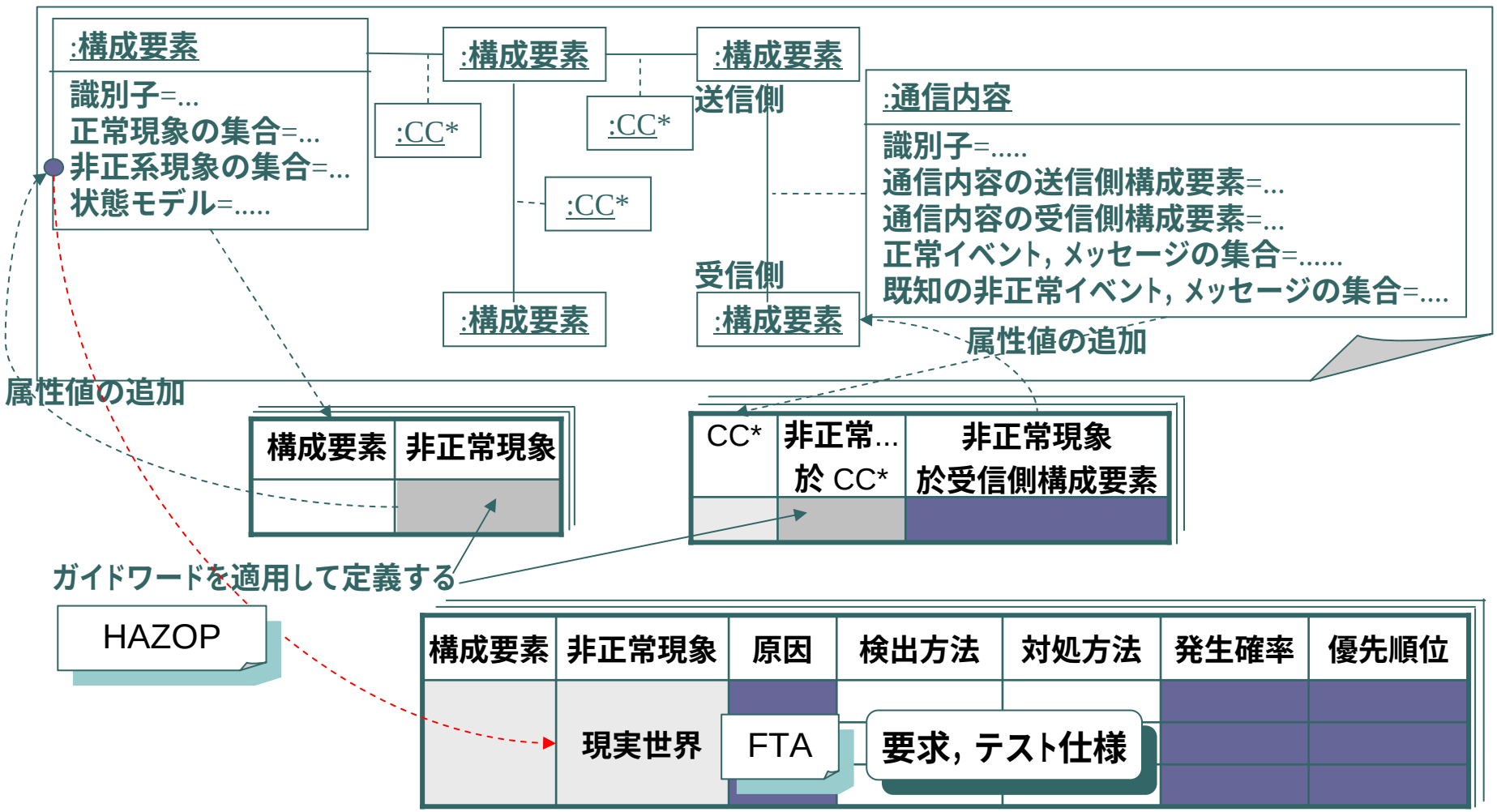
もう一つの試み

ESIM法：家電製品の安全性向上のための要求獲得技法

Toshiro MISE, Yasufumi SHINYASHIKI, Takako NAKATANI, Naoyasu UBAYASHI, Keiichi KATAMINE and Masaaki HASHIMOTO: "A Method for Extracting Unexpected Scenarios of Embedded Systems," Proc. of the JOINT CONFERENCE ON KNOWLEDGE-BASED SOFTWARE ENGINEERING 2006 (JCKBSE06).

現実世界とシステムへの要求

CC*：CommunicationContents（通信内容）



HAZOPの適用：代金投入（一部）における例外事象の抽出

1. アクターは紙幣投入口，硬貨投入口，プリペードカード読み取り機に手で貨幣を投入し，システムに渡す．
   - 1a.システムの処理能力以上の速さで貨幣が投入された場合
   - 1b.不正行為によって投入口、貨幣の通り道が詰まる。。。場合
   - 1c.取り出し口に商品が残っていて、あるいは、誤認識によって商品が取り出し口に残っていると、自販機が判断し、投入を許可できない場合
   - 1d.アクターが購入したい商品が売り切れになっていて、貨幣を投入するのをやめた場合

さいごに：：今後の要求工学

- これまでの経験によって，
  - 要求プロセス単体で，信頼性の高い，品質の高い要求仕様を得ることができないことは明らか．
  - 高い品質のシステムを得るために品質の高い要求仕様を定義しなければならないことも明らか．
- 統合型要求工学
  - 要求プロセスと開発プロセスの統合
  - 要求プロセスとテストプロセスの統合
  - 果たしてその効果は．．．．