ソフトウェア要求仕様における HAZOPを応用した リスク項目設計法

JaSST‘12 Tokyo
2012年1月25日(水)～26日(木)

株式会社 日立製作所
ソフトウェア事業部 品質保証部
河野 哲也

HITACHI
Inspire the Next

本研究のサマリ

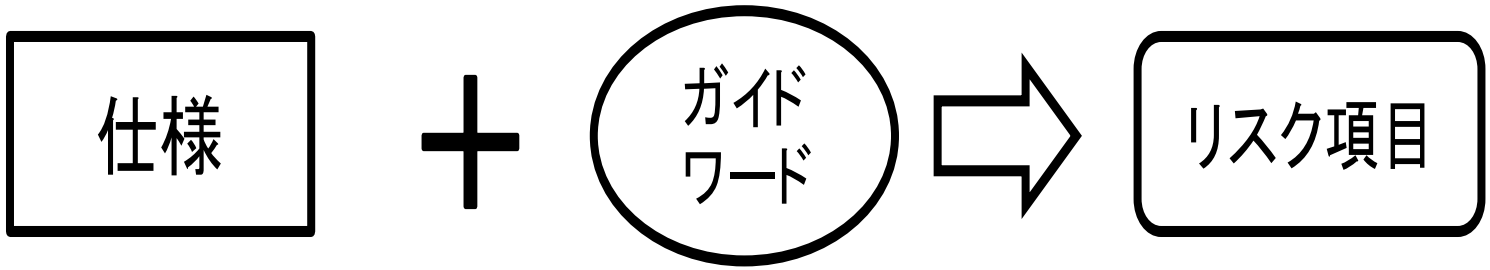
HITACHI
Inspire the Next

- 要求仕様を対象として
- HAZOPという
  リスク解析手法を応用して
- リスクを洗い出す方法の提案

本研究のサマリ

HITACHI
Inspire the Next

- USDMで記述された仕様に対して
- ガイドワードを組み合わせて
- リスク項目を洗い出す



ポイント

- プロダクトリスクを（徹底的に）洗い出す：リスク項目設計
- HAZOP：ガイドワード

発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

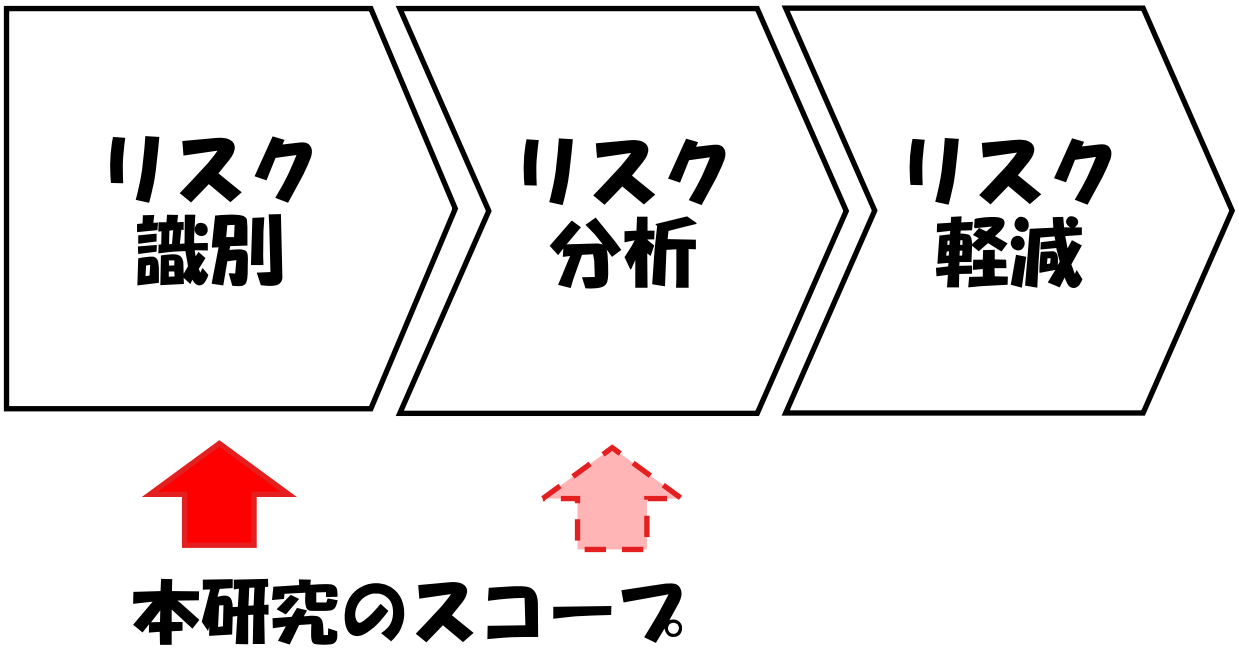
発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

イントロダクション

HITACHI
Inspire the Next

- リスクマネジメントは必要不可欠
  - 形式の差はあれ、どこの組織でも運用されている
- リスクマネジメントの3つの活動
  - リスク識別・リスク分析・リスク軽減



早くリスクを洗い出すことが重要

HITACHI
Inspire the Next

- 開発の早い段階で徹底的にリスクを洗い出すことが重要
  - ◆想定できないリスクは分析もできないし軽減策も立てれない
    - □最上流工程で作成される成果物、例えば要求仕様を徹底的にたたく必要がある
- リスクの洗い出しには多面的な視点が必要
  - ◆例えば、ユーザのシナリオをもとに考えたり品質特性から導き出したり過去の障害から連想したり
  - ◆HAZOPはリスク洗い出しの一視点を提供

HITACHI
Inspire the Next

●USDM：要求仕様の記述方法の一つ

◆システムクリエイツ 清水氏が提唱

◆要求と仕様を階層構造で表現する方法

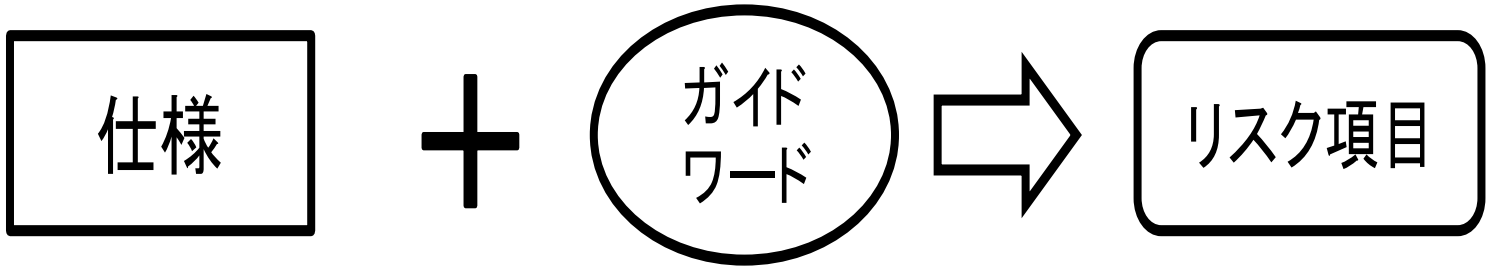
ロ仕様が項目として列挙される

要求1	受信した電子メールをキーワード検索したい		
	理由1	メールが多くて、関連するメールが探せない	
	要求1-1	検索対象のメールボックスを指定してグループ化できる	
		理由1-1	仕事上のメールとニュース等のメールを分けて扱いたい
		仕様1-1-1	メーラーが管理するメールボックスを一覧表示する
		…	…
		仕様1-1-4	一覧からメールボックスを選択したグループに指定する
	要求1-2	いくつかのキーワードを組み合わせて検索できる	
		理由1-2	可能性のあるキーワードで探したい
		仕様1-2-1	検索したいキーワードを入力できる

本研究のアプローチ

HITACHI
Inspire the Next

- **仕様：**
  USDMで記述された要求仕様の仕様
- **ガイドワード：**
  従来研究を応用し本研究で提示
- **＋と⇒：**
  リスク項目の設計として手順を整理



発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

HAZOPとは

HITACHI
Inspire the Next

- FMEA／FTAと並ぶ代表的なリスク解析法
  - ◆HAZard and OPerability study
    （潜在危険と運転性の解析手法）の略
  - ◆設計・運用の意図からの逸脱・ズレ（リスク）、
    それによって引き起こされる事故（影響）を解析する
    - ロ逸脱・ズレをガイドワードを利用して洗い出すのが特徴
- 主に化学プラントで適用されてきた手法
  - ◆流量や圧力などに対して「ない」「反対に」などの
    ガイドワードを組み合わせてリスクを洗い出す
    - ロリスクの例）「流量がない」「逆流する」など
  - ◆リスクに対して分析・評価する

HAZOPに関する従来研究

HITACHI
Inspire the Next

- ソフトウェアエンジニアリング分野
  - UMLや状態遷移図を対象とした研究
- 他分野
  - 医療分野
    - 医療行為のプロセスに対してHAZOPを適用
  - 一般消費者向け製品分野（例えば、電気コンロなど）
    - 不特定多数のユーザが使用する製品において エラーモードを網羅的に抽出するための取組み
    - ガイドワードの体系的な整理
      - 広辞苑から1120個の副詞を抽出し、整理を行った

発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

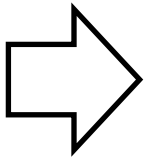
HITACHI
Inspire the Next

HAZOPの応用

HITACHI
Inspire the Next

●「動作」と仕様の「振舞い」と置き換え 従来のガイドワードを整理

ガイドワードの特徴		ガイドワード		
動作の量	動作の有無	全く～しない		
	動作の程度	強く	弱く	
	動作の速度	急いで	ゆっくり	
	持続時間	ずっと	短く（一時的に）	
	動作範囲	余分に	不十分に	
動作の向き	方向	反対に	他に	
	回転	反対に		
動作の種類		違う		
動作の対象	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	
時間		まだ	すでに	同時に
		別々に		
順序		前に	抜かして	後に
		余分に	繰り返し	反対に
回数		多く	少なく	



着目点		ガイドワード		
振舞いそのもの	有無	全く～しない		
	程度	強く	弱く	
	速度	急いで	ゆっくり	
	持続時間	ずっと	短く（一時的に）	
	範囲	余分に	不十分に	
	向き	反対に	他に	
	種類	違う		
	タイミング	遅く	早く	同時に
		別々に		
	順序	前に	抜かして	後に
		余分に	繰り返し	反対に
	回数	多く	少なく	
振舞いの対象	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	ない

本研究の考え方

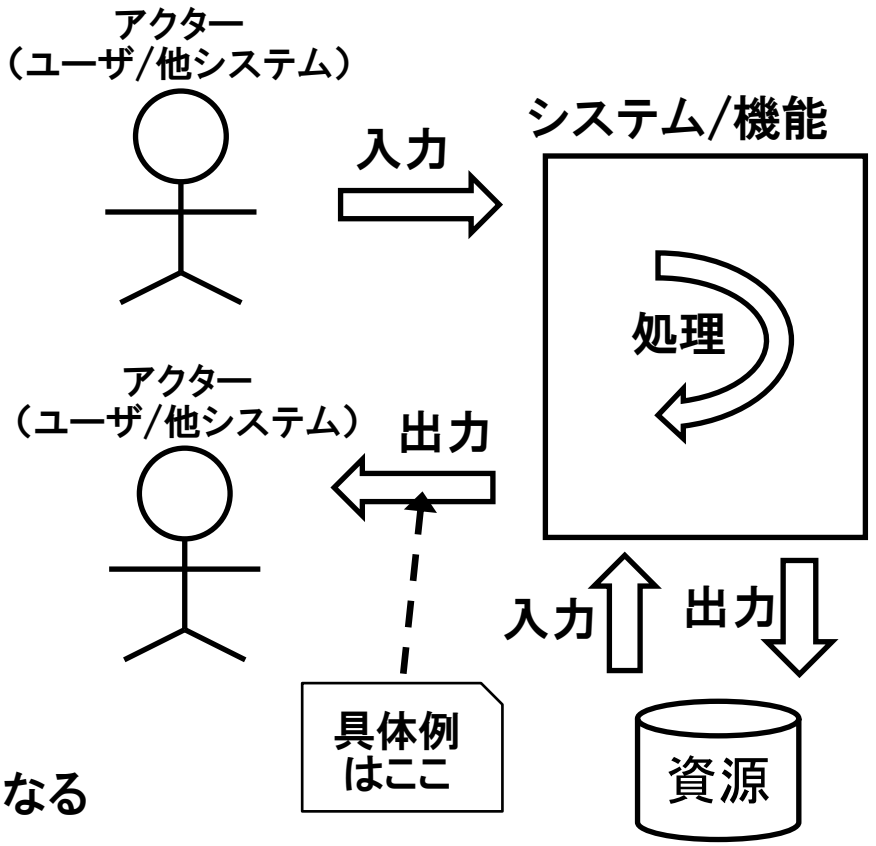
HITACHI
Inspire the Next

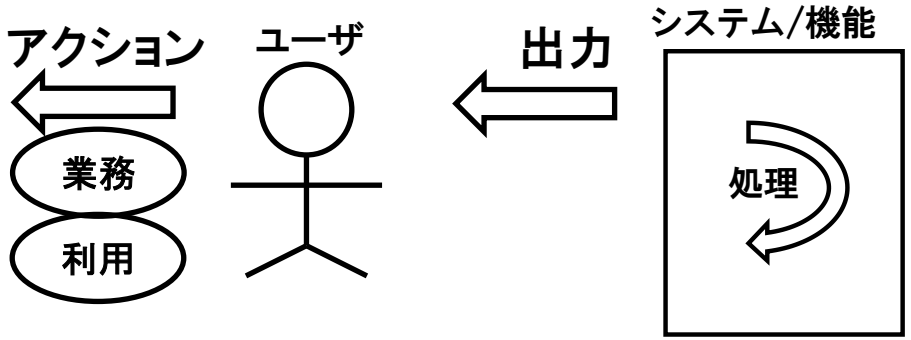
- 仕様に対しガイドワードを組み合わせて
  リスクを洗い出す

- 仕様「メールを一覧表示する」に対して
  ガイドワード「ゆっくり」を組み合わせると
  リスク項目「ゆっくり一覧表示する」が抽出される
  - ◆この抽出する行為を「リスク項目の設計」と呼ぶ

基本的な考え方

- 構造ビュー
  - ◆分析対象仕様がシステムの
    どの振舞いを対象としているのかを
    定めておく
    - ロ入力であればユーザの
      使い方を解析することになる
- 因果ビュー
  - ◆解析対象に対して因果の前後が
    どこかを定めておく
    - ロ具体例は出力を基点とし
      原因が処理、
      結果(影響)がユーザのアクションになる





提案手法の流れ

HITACHI
Inspire the Next

- 従来研究に従い、4つの手順で整理
  - 手順1：対象仕様の選定
  - 手順2：リスク項目の設計
  - 手順3：リスク項目の評価
  - 手順4：リスク項目の対策

- ガイドワードを使ってリスクを洗い出す作業は手順2で行う

手順1：対象仕様の選定

HITACHI
Inspire the Next

- 対象とする仕様項目を選定する
  - ◆要求の優先順位などに従い
    対象とする要求項目の選定を行い
    それに属する仕様項目に対しリスク項目を設計する
    - ロガイドワードの数にもよるが
      HAZOPをきっちりやると多くの時間を要するため

- べた書きの仕様の場合：
  仕様項目として特定の単位に整理する
  - ◆ガイドワードと組み合わせる仕様単位を用意する

手順2:リスク項目の設計

HITACHI
Inspire the Next

- リスク項目抽出表を作成する
  - ◆仕様項目とガイドワードを組み合わせた表

		仕様項目		
		検索されたメールの「Subject」を一覧で表示する	検索されたメールに連続番号を付けて表示する	・・・・・
ガイドワード	ない			
	早い			
	遅い			
	・ ・ ・ ・			

手順2:リスク項目の設計

HITACHI
Inspire the Next

- 仕様項目とガイドワードの交点に対して
  リスク項目案を抽出する
  - ◆正常な状態や振舞いに対しての逸脱・ズレを
    表現したものを書き出していく

		仕様項目		
		検索されたメールの「Subject」を一覧で表示する	検索されたメールに連続番号を付けて表示する	・・・・・
ガイドワード	ない	・・・・・	番号が付かずに表示される	・・・・・
	早い	すばやく表示される	・・・・・	・・・・・
	遅い	遅く表示される	・・・・・	・・・・・
	・ ・ ・ ・	・・・・・	・・・・・	・・・・・

手順2:リスク項目の設計

HITACHI
Inspire the Next

- リスク項目案からリスク項目を選択する
  - ◆ユーザへの影響などを考慮し、望ましくない影響を及ぼすものをリスク項目として採用する
    - ロ例えば、「遅く表示される」というリスク項目案に対してユーザの業務に遅延が生じるという影響が想定されればリスク項目として採用する

		仕様項目		
		検索されたメールの「Subject」を一覧で表示する	検索されたメールに連続番号を付けて表示する	・・・・・
ガイドワード	ない	・・・・・	番号が付かずに表示される	・・・・・
	早い	すばやく表示される	・・・・・	・・・・・
	遅い	遅く表示される	・・・・・	・・・・・
	・ ・ ・ ・	・・・・・	・・・・・	・・・・・

手順3:リスク項目の評価

HITACHI
Inspire the Next

- リスク項目を列挙しリスク評価を行うためのシートを作成する
  - ◆FMEA表に近い形式

リスク項目	影響	想定原因	影響度	発生可能性	リスク度	対策
「Subject」の一覧が遅く表示される						
検索されたメールに番号が付かずに表示される						
・・・・・						

手順3:リスク項目の評価

HITACHI
Inspire the Next

- 各リスク項目の影響と想定原因を検討する
- 各リスク項目に対して影響度と発生可能性の指標を用いてリスク度を算出し対策の可否を判断する

リスク項目	影響	想定原因	影響度	発生可能性	リスク度	対策
「Subject」の一覧が遅く表示される	業務が遅延する	表示時に並列で検索を走らせている	3	3	9	メール検索の並列処理を禁止する
検索されたメールに番号が付かずに表示される	・・・・・	・・・・・	・・・	・・・	・・・	・・・
・・・・・	・・・・・	・・・・・	・・・	・・・	・・・	・・・

手順4:リスク項目の対策

HITACHI
Inspire the Next

- 対策を実施すると判断したリスク項目に対して具体的な対策案を立案・計画する
  - ◆仕様変更や機能追加、マニュアル変更などの抜本的解決によるリスク対策
    - ロフェールセーフやエラープルーフなどの適用
  - ◆設計や実装などの各タイミングでのレビュー観点の用意、およびその実施、実施結果の記録
  - ◆テスト項目への反映および動作確認、その実施結果の記録

発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

検証の概要

HITACHI
Inspire the Next

- USDMで記述された電子メールの仕様に対して
  リスク項目の設計を行う
  - ◆手法を使用するグループ(手法使用グループ)と
    手法を使用せず経験的なグループ(経験ベースグループ)
    の2つのグループによって実施
    - ロ手法使用グループ:若手エンジニア2名
    - ロ経験ベースグループ:ベテランエンジニア2名
  - ◆両グループともに、リスク項目案の抽出は個人で
    リスク項目の選定はグループで実施
  - ◆設計されたリスク項目に対して比較・評価を行う

手法使用グループの詳細

HITACHI
Inspire the Next

- 手法使用グループが利用したリスク項目抽出表
  - ◆仕様項目3×ガイドワード29
  - ◆87項目に対してリスク項目案を抽出した
  - ◆お互いのリスク項目案に対して検討を進めリスク項目の選択を行う

【手法使用グループ配布】			<検索件数の表示> 仕様1 検索されたメールの件数を一覧の上に表示する	<検索メールの表示> 仕様2 検索されたメールの「Subject」を一覧で見せる	仕様3 検索されたメールに連続番号を付けて表示する	仕様4 検索されたメールの件数10件を超えるときはスクロールバーを表示する
振舞いそのもの	振舞いの有無	全く～しない	1			1
	振舞いの程度	強く	2		2	2
		弱く	3		3	3
	振舞いの速度	急いで	4		4	4
		ゆっくり				
	持続時間	ずっと				
		短く（一時的に）				
	動作範囲	余分に	8		8	8
		不十分に	9		9	9
	向き	反対に	10		10	10
		他に	11		11	11
	種類	違う	12		12	12
	タイミング	遅く	13		13	13
		早く	14		14	14
		同時に	15		15	15
		別々に	16		16	16
	順序	前に	17		17	17
		抜かして	18		18	18
		後に	19		19	19
		余分に	20		20	20
		繰り返し	21		21	21
		反対に	22		22	22
	回数	多く	23		23	23
		少なく	24		24	24
振舞いの対象	対象物	違うものに	25		25	25
	対象物の向き	反対に	26		26	26
	対象物の量	多く	27		27	27
		少なく	28		28	28
		ない	29		29	29

検証結果

HITACHI
Inspire the Next

- 抽出されたリスク項目案

グループ	実験協力者	仕様1	仕様3	仕様4
経験ベース	A1	9項目	11項目	10項目
	A2	9項目	9項目	7項目
手法使用	B1	29項目	29項目	29項目
	B2	25項目	26項目	25項目

- 設計されたリスク項目数

グループ	仕様1	仕様3	仕様4
経験ベース	14項目	18項目	13項目
手法使用	22項目	27項目	22項目

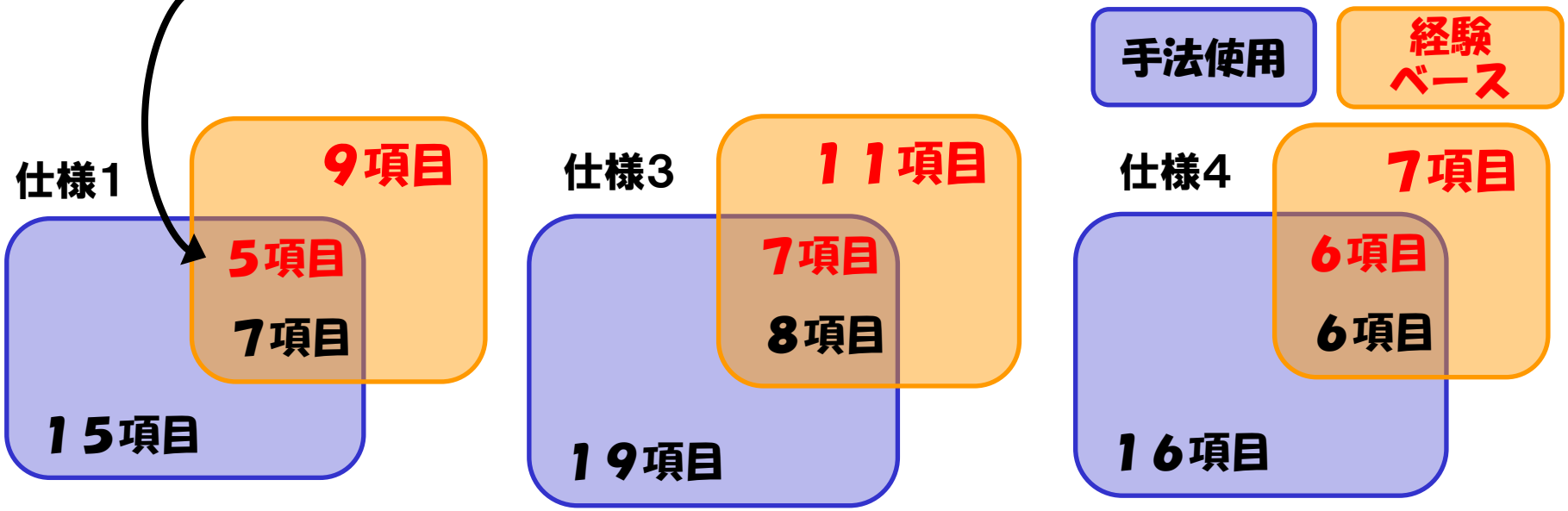
検証結果

HITACHI
Inspire the Next

- リスク項目の包含関係
  - ◆ 重複しない項目が多くみられる
  - ◆ 1項目同士の対応にならないもがあった

グループ	重複の有無	仕様1	仕様3	仕様4
経験ベース	しない	9項目	11項目	7項目
	する	5項目	7項目	6項目
手法使用	しない	15項目	19項目	16項目
	する	7項目	8項目	6項目

- 例えば、「件数が表示されない（常に0や空白）」に対して「件数が空白で表示される」と「件数が0で表示される」という対応



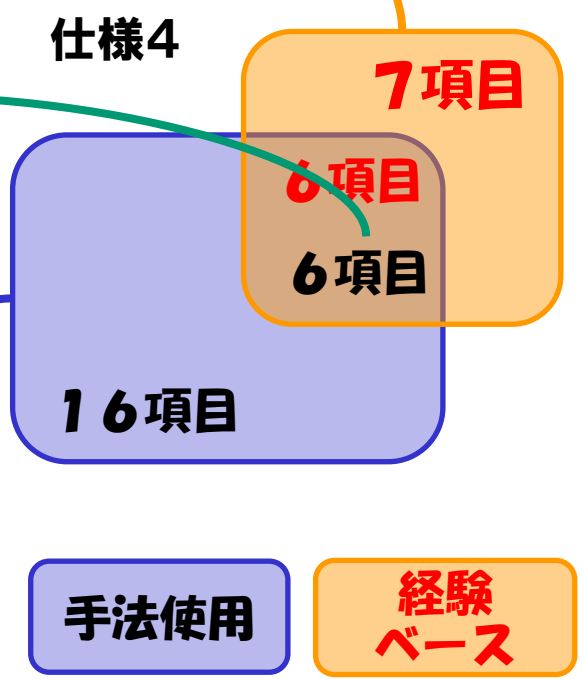
包含関係と具体例

HITACHI
Inspire the Next

•スクロールバーを動かしても一覧が動かない
•一度スクロールバーを表示すると再検索で
10件以下になっても消えない

•10件以上でもスクロールバーが表示されない
•10件以下でスクロールバーが表示される
•スクロールバーが動かない

•スクロールバーの表示位置が違う
•スクロールバーの表示タイミングが遅い
•スクロールする範囲が不十分



考察:有効性の評価

HITACHI
Inspire the Next

- 経験ベースグループ(ベテランエンジニア2名)が設計できなかった項目に対してヒアリングを実施した
  - ◆リスク識別として取り上げる必要があるかどうかを確認

グループ	重複の有無	仕様1	仕様3	仕様4
経験ベース	しない	9項目	11項目	7項目
	する	5項目	7項目	6項目
手法使用	しない	15項目	19項目	16項目
	する	7項目	8項目	6項目

- 評価結果
  - ◆仕様1では2項目、仕様3では6項目、仕様4では3項目を取り上げる必要があると2名ともが判断した
  - ◆例えば、「遅く表示される」や「小さく表示される」など
- 手法使用グループに限られるリスク項目のうち少数ではあるものの、有効と考えられるリスク項目がみられた

発表の流れ

- 背景・導入
- HAZOPとは
- 提案手法
- 検証
- まとめと今後の課題

まとめと今後の課題

HITACHI
Inspire the Next

- 発表の振り返り
  - ◆リスク識別、特にリスクの洗い出しに焦点を当てた
  - ◆仕様：USDMで記述された要求仕様の仕様
  - ◆ガイドワード：従来研究を応用し本研究で用意
  - ◆＋と⇒：リスク項目の設計として手順を整理

- 今後の課題
  - ◆ガイドワードの整備
  - ◆実プロジェクトへの適用とＦＴＡへの活用

END　ご静聴ありがとうございました

ソフトウェア要求仕様におけるHAZOPを応用した
リスク項目設計法

JaSST‘12 Tokyo

株式会社 日立製作所
ソフトウェア事業部 品質保証部
河野 哲也

HITACHI
Inspire the Next