

Case Study

File Sharing service KFSの アシュランスケース

2014年 12月 18日

神奈川大学 総合理学研究所
客員研究員 平井 誠

目次

- 目的
- 課題：関係者間の誤解・認識不足→整合性低下
- 取組1：DEOSサイクルに基づくアシュランスケースのフレームワーク(テンプレート)による認識の統一
- 取組2：形式アシュランスケースを用いた、関係者間の誤解・認識不足の検知・是正
- 考察：取組の費用と効果と、その改善にむけて
- まとめ

目的

- 【目的】 DEOSライフサイクルモデルと、その形式アシュランスケースの妥当性確認
 - 実システムを開発・運用し、上記の効果や課題を抽出し、改善を継続。
- 公開可能なアシュランスケースを得る。

課題

- 関係者全員の合意、アシュランスケース全体の整合性を維持する手法の開発
- 解決されるべき問題点：
 - 関係者間での用語の解釈の不統一からくるアシュランスケース記述内容の誤解
関係者（責任者・管理者・開発者・運用者・利用者）
 - アシュランスケース各部の記述・合意・承認・変化対応
分担からくる全体での不整合発生

取組1： フレームワークを用いた認識の統一

- DEOSに基づくOSDアシュランス記述の枠組み
 - ソフトウェアフレームワークの考え方
 - (DEOSサイクル:オープンシステムのディペンダビリティ(OSD)を実現するライフサイクルモデル)
- フレームワークとその具体化の取組ステップ
 - STEP1:一般的なOSDアシュランスケースのフレームワーク(枠組み)を定義
 - STEP2:特定分野、関係者組織形態に特化したフレームワーク定義
 - STEP3:特定のシステム、特定の関係者組織への具体化

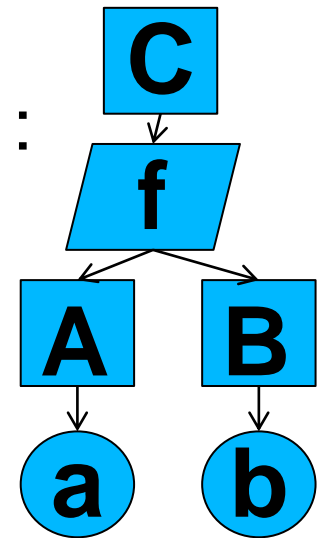
取組1： フレームワークの効果

- 記述分担による個人差低減
 - 記述すべき内容の漏れ防止
 - 仮合意・未決事項の管理効率向上
- 記述事例：
- 「検討中：xx担当yymmddまで」
 - 「記述不要：常識」
(その担当者には常識でも、ほかの担当者が見て、分析が必要だと、検知できる)

取組2:

形式アシュランスケース手法の適用

- **形式アシュランスケース**
= 合意された形式理論 & 検査済み形式証明
- **証明 = 主張の証拠となるデータを作るプログラム**
 - ○証拠 → データ
 - □主張 → 認めうる証拠データの集合(型)
 - ◇議論 → 証拠データを作るプログラム
- **証明の一例として、以下のように主張できる:**
 - □Aに○a、□Bに○bという証拠があり、
 - □Aと□Bから□Cを導く議論◇fがあれば、
 - □Cに○c(=◇f ○a ○b)という証拠がある。



取組2: 形式的議論断片

○(ファイル共有サービス)のアシュランスケース =

□(ファイル共有サービス)は適切である

⇒

◇合意形成と説明責任遂行と障害対応と
変化対応が適切ならば、サービスは適切

○(ファイル共有サービス)の合意形成は適切

○(ファイル共有サービス)の障害対応は適切

○(ファイル共有サービス)の変化対応は適切

○(ファイル共有サービス)の説明責任遂行は適切

具体的サービスについて記述

取組2: 形式的フレームワーク断片

○(ServiceX)のアシュランスケース =

□(ServiceX)は適切である

⇒

◇合意形成と説明責任遂行と障害対応と
変化対応が適切ならば、サービスは適切

○(ServiceX)の合意形成は適切

○(ServiceX)の障害対応は適切

○(ServiceX)の変化対応は適切

○(ServiceX)の説明責任遂行は適切

パラメータ化しフレームワーク作成

取組2-1: 語彙定義の共通化

以下等に関する語彙を共通化し、誤解を低減

- 議論されるべき事柄、網羅されるべき事項のリスト
- 証拠データ(証拠文書へのタグ)
ニーズ分析書、要件定義書、設計書、テスト設計書兼結果書、利用手順書、運用手順書
- 前提データ(前提文書へのタグ)
プロバイダ資料、情報管理規定、Linuxマニュアル

最上位の主張から始めて、段階的に、議論されるべき事柄についての主張に分解し、定義された証拠や前提に到達するまで分解。

取組2-1: DEOS共通語彙

DEOSライフサイクルで議論されるべき事柄を共通化

- 合意形成
- 障害対応
- 変化対応
- 説明責任遂行

取組2-1: 障害対応の語彙

議論すべき対象(システムに依存)を共通化
(変化対応により更新されうる)

- ファイルサーバ停止
- ファイル喪失
- ファイルサーバ喪失

取組2-1: 変化対応事例

1. 開発担当者が新規に対応すべき障害を障害リストに追加。開発関連のアシュランスケースを更新。
2. アシュランスケース全体で整合性検査実施。共通の障害リストを更新したため、運用関連のアシュランスケースで、障害リストを網羅した議論ができていないことが判明。
3. 運用担当者が開発担当者と連絡して、運用関連のアシュランスケースにも新規に対応すべき障害に関する議論を追加。
4. アシュランスケース全体での整合性確認。

取組2-1 : Agdaによる記述例(1/4)

議論項目の語彙

```
emacs@MACHIRAI-VAIO
File Edit Options Buffers Tools Agda Help
module FailureResponse where
  --Ontology
  --アシュランスケースで議論する特定のシステムやサービスのリスト
  data System : Set where KFS : System

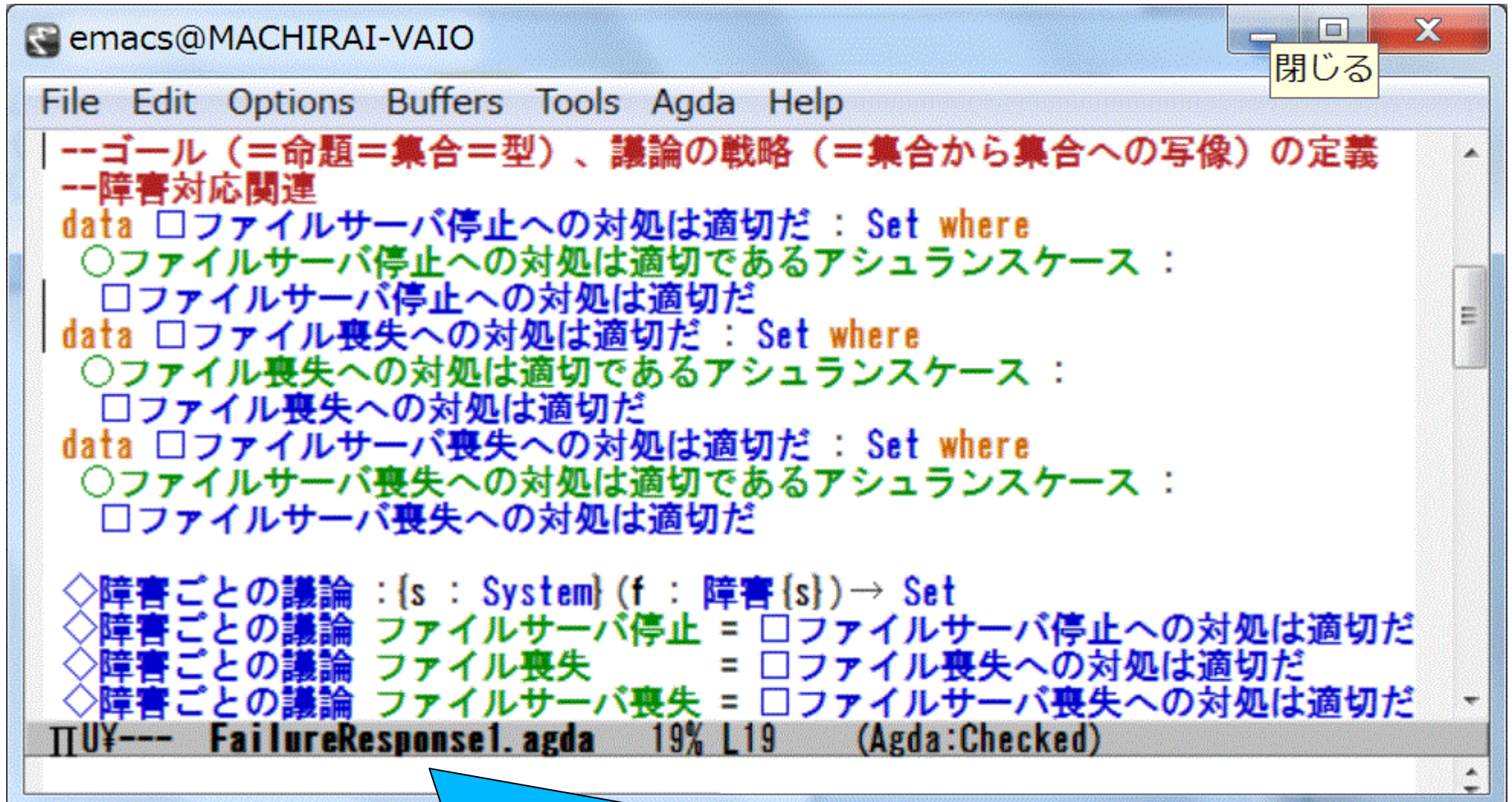
  --議論で網羅すべき対象のリスト (特定のシステムに依存する)
  data DEOSview{s : System}: Set where
    合意形成 障害対応 変化対応 説明責任遂行 : DEOSview

  data 障害{s : System}: Set where
    ファイルサーバ停止 ファイル喪失 ファイルサーバ喪失 : 障害

  --命題 (=ゴール=集合=型) に証拠 (=その型のデータ=その集合の要素) を
  --与える演算子 _○_
  _○_ : (□Goal : Set) → □Goal → □Goal
  □Goal ○ evidence = evidence
[]UY--- FailureResponse1.agda Top L12 (Agda:Checked)
```


取組2-1 : Agdaによる記述例(2/4)

障害対応の語彙



```
emacs@MACHIRAI-VAIO
File Edit Options Buffers Tools Agda Help
--ゴール (=命題=集合=型)、議論の戦略 (=集合から集合への写像) の定義
--障害対応関連
data □ファイルサーバ停止への対処は適切だ : Set where
  ○ファイルサーバ停止への対処は適切であるアシュランスケース :
    □ファイルサーバ停止への対処は適切だ
data □ファイル喪失への対処は適切だ : Set where
  ○ファイル喪失への対処は適切であるアシュランスケース :
    □ファイル喪失への対処は適切だ
data □ファイルサーバ喪失への対処は適切だ : Set where
  ○ファイルサーバ喪失への対処は適切であるアシュランスケース :
    □ファイルサーバ喪失への対処は適切だ

◇障害ごとの議論 : {s : System} (f : 障害{s}) → Set
◇障害ごとの議論 ファイルサーバ停止 = □ファイルサーバ停止への対処は適切だ
◇障害ごとの議論 ファイル喪失 = □ファイル喪失への対処は適切だ
◇障害ごとの議論 ファイルサーバ喪失 = □ファイルサーバ喪失への対処は適切だ
IIUY--- FailureResponse1.agda 19% L19 (Agda:Checked)
```

議論を深めていく途中段階の証拠を含む

取組2-1：Agdaによる記述例(3/4)

DEOSサイクルの語彙

```
emacs@MACHIRAI-VAIO
File Edit Options Buffers Tools Agda Help
--DEOSサイクル関連
data  合意形成は適切だ : Set where
  ○ 合意形成は適切であるアシュランスケース :  合意形成は適切だ
data  障害対応は適切だ : Set where
  ○ 障害対応は適切であるアシュランスケース :  障害対応は適切だ
data  変化対応は適切だ : Set where
  ○ 変化対応は適切であるアシュランスケース :  変化対応は適切だ
data  説明責任遂行は適切だ : Set where
  ○ 説明責任遂行は適切であるアシュランスケース :  説明責任遂行は適切だ

◇ DEOS議論 : {s : System} (d : DEOSview{s}) → Set
◇ DEOS議論 合意形成 =  合意形成は適切だ
◇ DEOS議論 障害対応 =  障害対応は適切だ
◇ DEOS議論 変化対応 =  変化対応は適切だ
◇ DEOS議論 説明責任遂行 =  説明責任遂行は適切だ

IIUY--- FailureResponse1.agda 43% L40 (Agda:Checked)
```

議論を深めていく途中段階の証拠を含む

取組2-1: Agdaによる記述例(4/4)

形式アシュランスケース

emacs@MACHIRAI-VAIO

File Edit Options Buffers Tools Agda Help

-- アシュランスケース (= トップゴールの証明 = 集合の要素を与えるプログラム)

- 障害対応は適切であるアシュランスケース1 : \square 障害対応は適切だ1
- 障害対応は適切であるアシュランスケース1 = $(\forall \{s : \text{System}\} \{f : \text{障害}\{s}\} \rightarrow$
 - ◇ 障害ごとの議論 f) ○
 - 障害ごとの議論 where
 - 障害ごとの議論 : $\{s : \text{System}\} \{f : \text{障害}\{s}\} \rightarrow$ ◇ 障害ごとの議論 f
 - 障害ごとの議論 [KFS] {ファイルサーバ停止} =
 - ファイルサーバ停止への対処は適切であるアシュランスケース
 - 障害ごとの議論 [KFS] {ファイル喪失} =
 - ファイル喪失への対処は適切であるアシュランスケース
 - 障害ごとの議論 [KFS] {ファイルサーバ喪失} =
 - ファイルサーバ喪失への対処は適切であるアシュランスケース
- KFSのDEOSサイクルの遂行は適切 : \square DEOSサイクルの遂行は適切だ
- KFSのDEOSサイクルの遂行は適切 = $(\forall \{s : \text{System}\} \{d : \text{DEOSview}\{s}\} \rightarrow$
 - ◇ DEOS議論 d) ○
 - DEOS議論 where
 - DEOS議論 : $\{s : \text{System}\} \{d : \text{DEOSview}\{s}\} \rightarrow$ ◇ DEOS議論 d
 - DEOS議論 [KFS] {合意形成} = ○ 合意形成は適切であるアシュランスケース
 - DEOS議論 [KFS] {障害対応} = ○ 障害対応は適切であるアシュランスケース
 - DEOS議論 [KFS] {変化対応} = ○ 変化対応は適切であるアシュランスケース
 - DEOS議論 [KFS] {説明責任遂行} = ○ 説明責任遂行は適切であるアシュランスケース

取組2-2: 障害対応の網羅確認

議論すべきアクションを共通化

- 予防:(例)ファイルのバックアップ
- 検知:(例)ファイルサーバの監視
- 緊急対応:(例)喪失の原因究明と対応
- 減災復旧:(例)バックアップからの復旧
- 記録:(例)説明責任遂行に十分な記録

取組2-2: 障害と障害対応の網羅確認

	ファイルサーバ停止	ファイル喪失	ファイルサーバ喪失
予防	実績のあるサーバを選択	バックアップ	実績のあるサーバを選択
検知	業者の連絡	サーバの監視	サーバの監視
緊急対応	バックアップからの提供	サーバ停止 ウイルス除去	バックアップからの提供
減災復旧	停止中の更新のアップロード	バックアップからの復旧	バックアップからの復旧
記録	停止連絡、バックアップからの提供メール	ファイル更新記録、復旧記録	喪失原因と経緯の連絡記録

取組2-3: 5W1H網羅確認

議論すべき項目のリスト(5W1H)を共通化

- Why:(例)長くても6時間前の状態に復帰、サーバと同じ災害を避ける
- Where:(例)サーバとは別の場所で
- Who:(例)常時動作しているコンピュータが
- When:(例)6時間ごとに
- What:(例)更新されたファイルの差分を
- How:(例)転送後チェックサムを確認して保存
管理者に、バックアップ状況報告メール送信

取組2-3: 障害対応のタイムライン確認

ID	Who	When	How(long)	What
1	管理者	6時間ごと	6時間以内	監視結果をチェック、2へ
2	管理者	異常検知後	1時間以内	責任者へ報告、3へ
3	管理者	異常検知後	2時間以内	利用者へ報告、4へ
4	管理者	異常検知後	3時間以内	原因究明・緊急対応、5へ
5	管理者	緊急対応後	1時間以内	責任者へ報告、6へ
6	管理者	緊急対応後	1時間以内	利用者へ報告、7へ
7	利用者	報告受信後	1日以内	バックアップ利用申請
8	管理者	利用申請後	1時間以内	バックアップ提供
9	管理者	緊急対応後	1日以内	バックアップから復旧、10へ
10	管理者	復旧後	1時間以内	責任者へ報告、11へ
11	管理者	復旧後	1時間以内	利用者へ報告

取組2-n: 語彙定義の共通化(再掲)

以下等に関する語彙を共通化し、誤解を低減

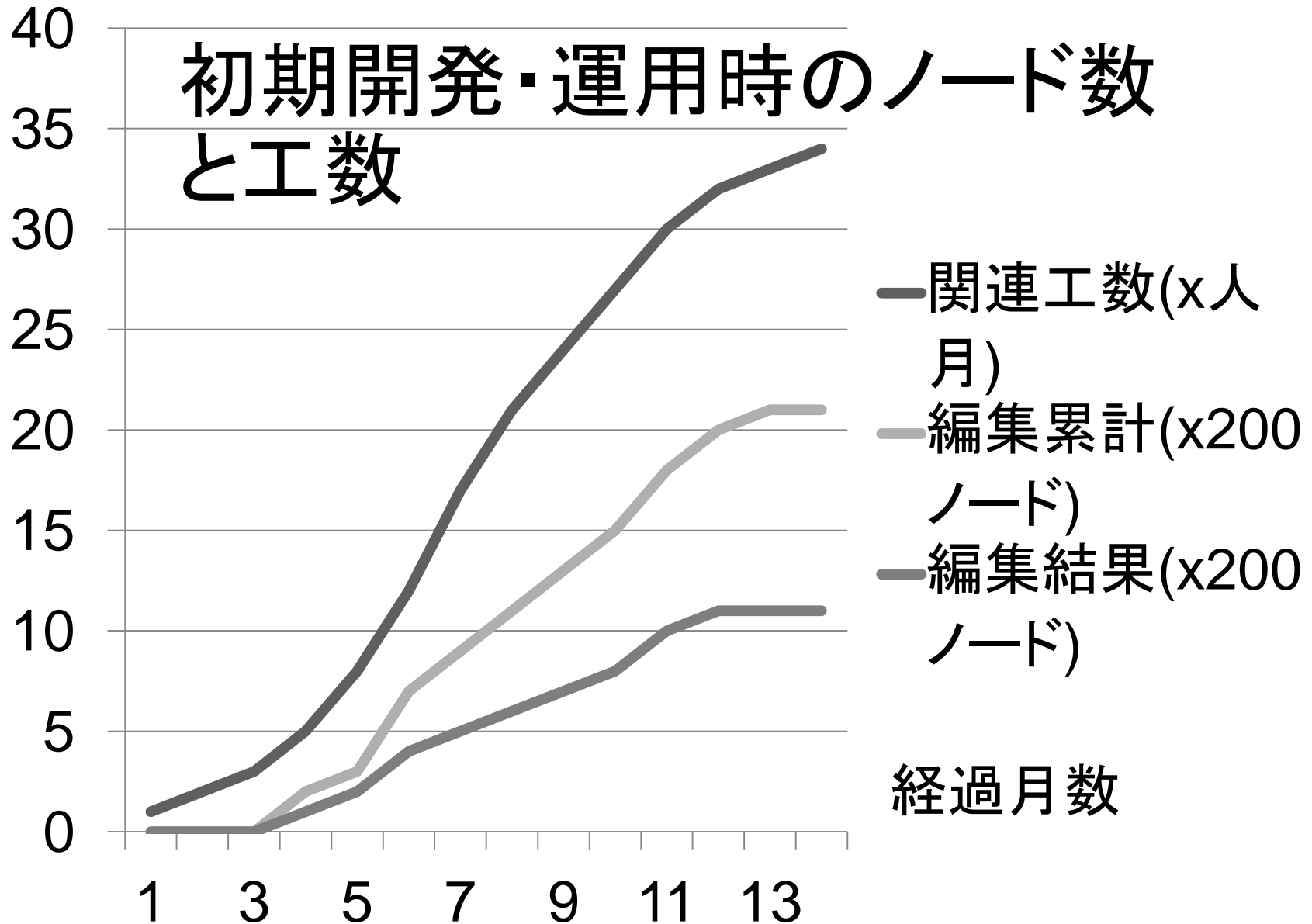
- 議論されるべき事柄、網羅されるべき事項のリスト
- 証拠データ(証拠文書へのタグ)
ニーズ分析書、要件定義書、設計書、テスト設計書兼結果書、利用手順書、運用手順書
- 前提データ(前提文書へのタグ)
プロバイダ資料、情報管理規定、Linuxマニュアル

最上位の主張から始めて、段階的に、議論されるべき事柄についての主張に分解し、定義された証拠や前提に到達するまで分解。

考察： 取組を通じての効果

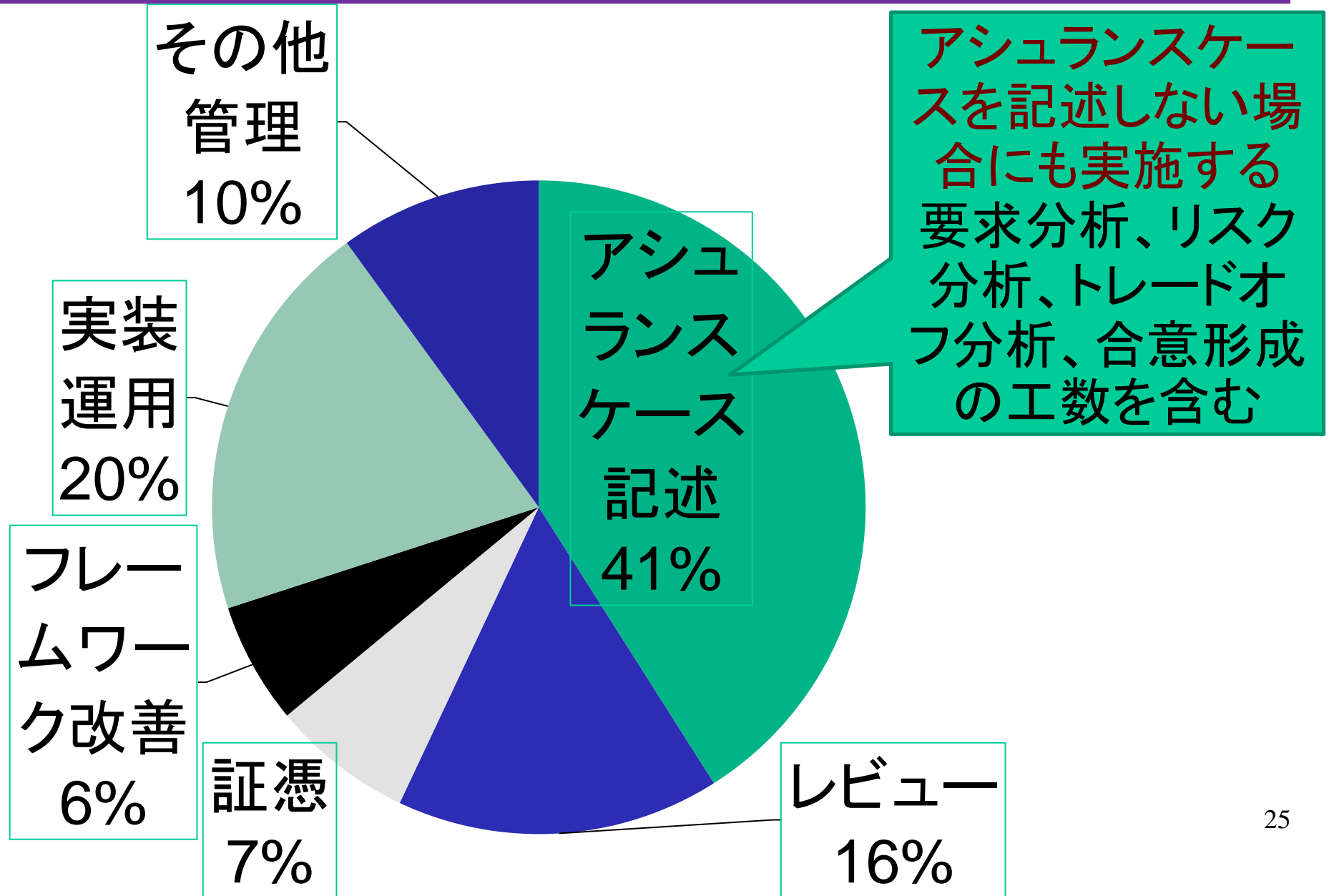
- ニーズ・仕様・利用方法・運用方法を共有
語彙を明確化し、誤解を低減
- 一度合意したアシュランスケースの整合性維持
仮合意（常識、未定義、低優先度により未検討）
バックログ、不具合・バグレポートをレビュー
⇒アシュランスケースを効率よく改定しつつ、
システムや利用・運用方法を確実に改善
- 網羅すべき項目のリストを用いて、整合性を自動
検査

考察： 取組の費用



考察:

アシュランスケース記述工数の割合



考察： 取組の改善にむけて

- フレームワークの積み上げ、改定継続中
→出来上がったフレームワークを利用した
変化対応工数は、習熟とともに、減少傾向
- 今後：
 - アシュランスケースの出来栄を評価し、改定していくための基準
(段階的基準：優先順位を考慮し段階的に作成)
 - 評価ツールとしてのメタアシュランスケース

まとめ

- 関係者で分担してアシュランスケースを記述。
誤解を低減していくための
フレームワークとその形式モデルの例を紹介。
- ・議論対象のリストを用いて整合性を検査。
- 今後の課題：
アシュランスケース評価の基準とツール
-どこまで階層的に掘り下げて議論するか？
-関係者での合意・教育・訓練の維持は十分か？