Empowered by Innovation NEC

「話題沸騰ポット(GOMA-1015型)テスト設計

～安全なポットを使っていただくために～

チームｎｅｍａ
ID:1320008

目次

- はじめに
- テスト設計の位置づけ
- テスト戦略
- 安全性のための要求分析
- テスト設計（機能視点テスト）
- テスト設計（ユーザ視点テスト）
- さいごに

はじめに

はじめに

チームについて

- チーム名：チームｎｅｍａ
- メンバー：

  根間 才治、小池 輝明、葛西 孝弘、下前 真浩、鬼頭 素子、岩崎 雅子
  山口 元人、春田 恒一良
- 概要・活動：
  - ＮＥＣのＳＷＱＣ活動(全社的なソフトウェア開発改善活動)コミュニティのひとつ「テスト技術者交流会」を母体とするメンバー
  - コミュニティとして、テスト技術の向上とＮＥＣグループ内への普及・展開を目的に鋭意活動中

  主な活動実績：
    - 結合テストにおけるテスト観点のヌケモレ防止を目的とした「テスト設計テンプレート」の作成とＮＥＣグループ内への展開（JaSST Tokyoでも事例発表）
    - ＮＥＣグループ向けテスト技術シンポジウム開催
    - テスト設計コンテスト参加（JaSST'12 Tokyo）

テスト設計について

- 本テスト設計は、「話題沸騰ポット(GOMA-1015型)要求仕様書(第７版)に基づき開発される電気ポットのソフトウェアについてテストを実施するためにテスト設計したものである。

テスト設計方針

テスト設計にあたって ～安全性の追求～

市場における製品事故の再発をソフトウェアテストで防止する

- 実際に発生した事故事例を調査・分析する
- 調査対象：下記団体が公表している事例
  - 調査機関：製品評価技術基盤機構 (NITE) や消費者センターなど
  - 行政機関：消防や経済産業省など
  - 各製造メーカー

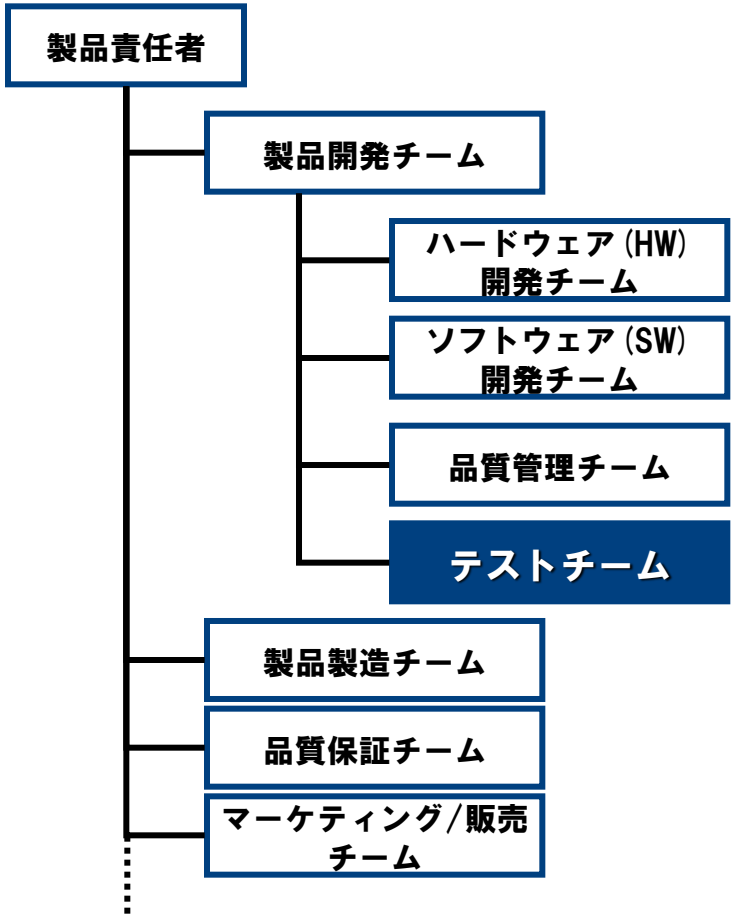
事故事例を回避するための２つのテスト

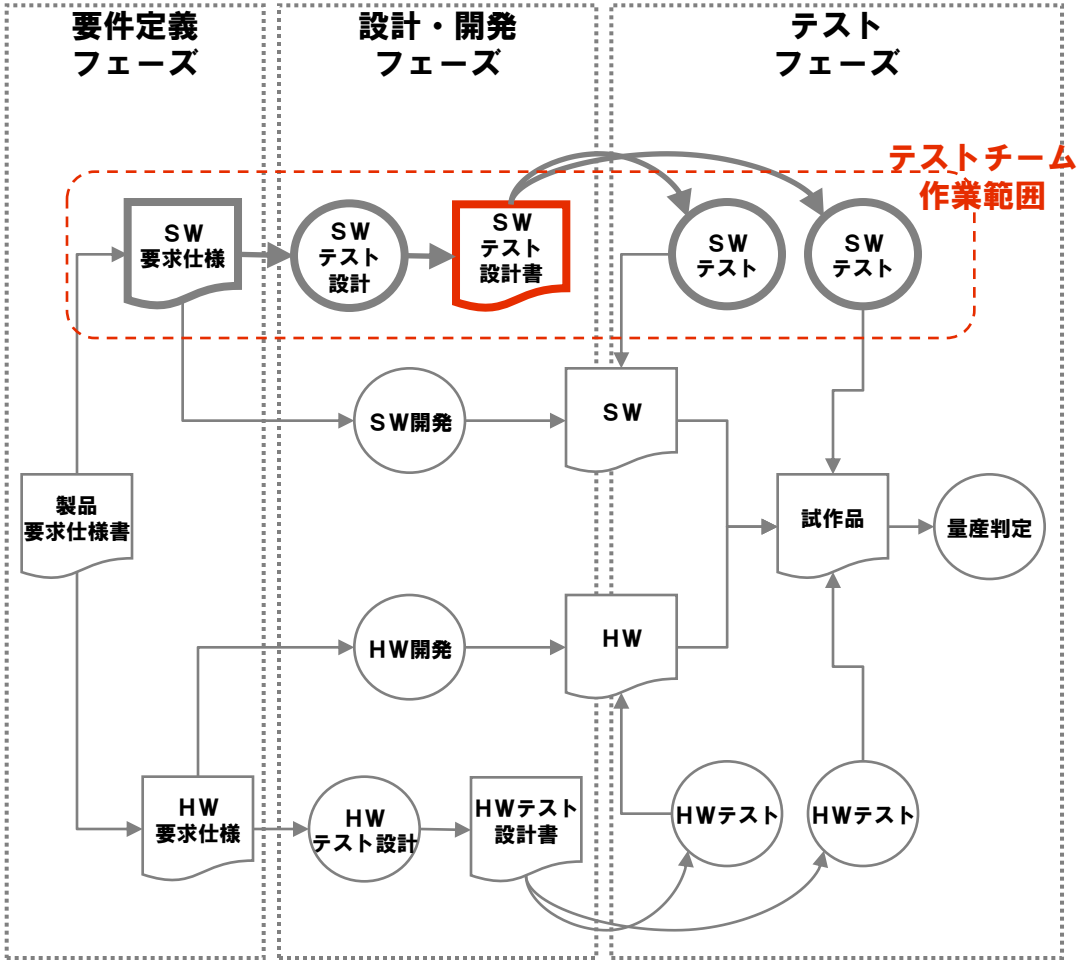
- ＳW開発時テスト：要求仕様から導いた「機能視点テスト」
- 量産前テスト：事故事例から導いた「ユーザー視点テスト」

テスト設計の位置づけ

開発体制・開発プロセス

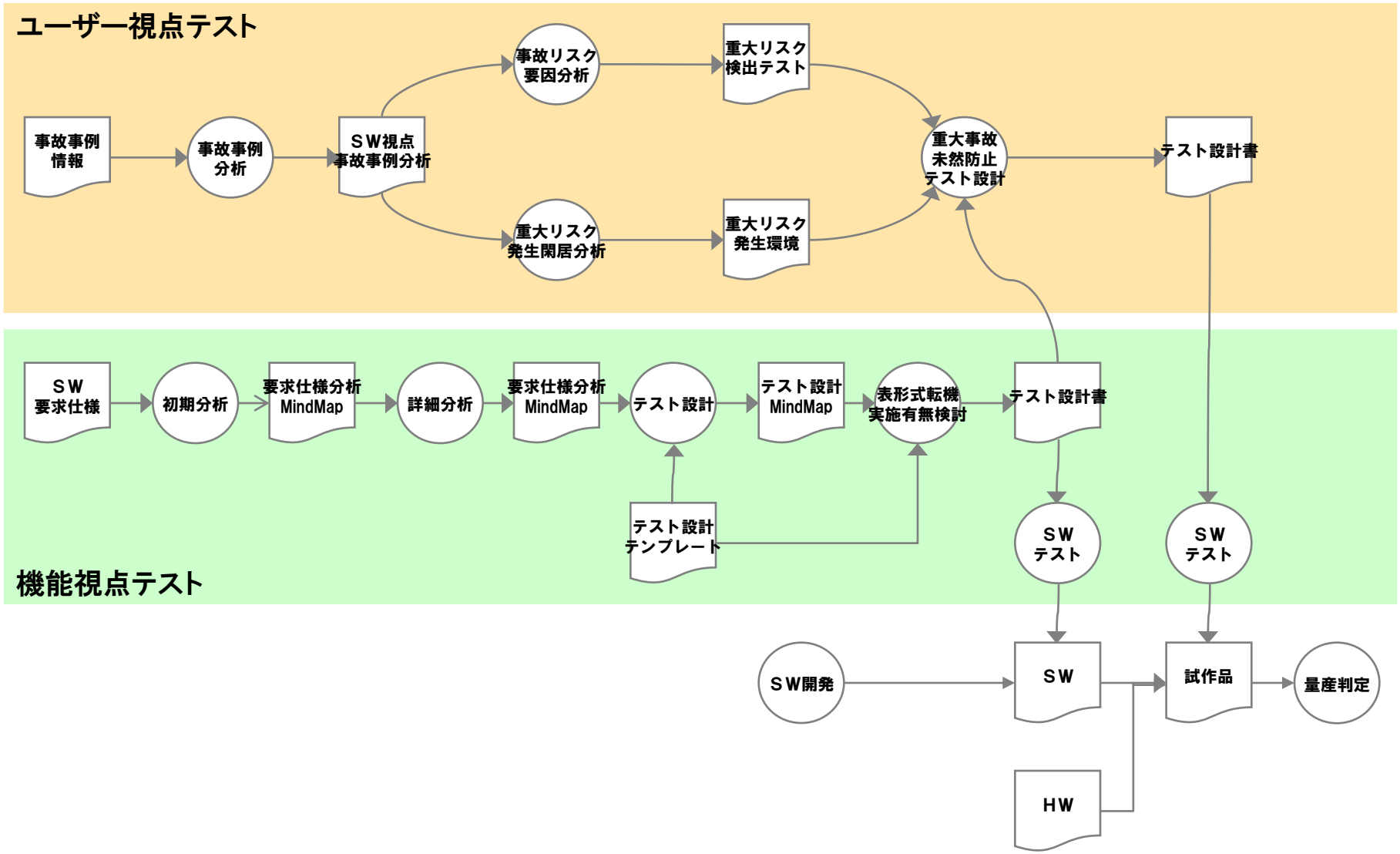
今回のテスト設計を行うにあたって、対象製品の開発体制と開発フェーズ、開発プロセスを以下のように設定する。今回のテスト設計書は、テストチームから各チームに対してテストの妥当性を確認してもらう「テスト設計レビュー」で用いられる





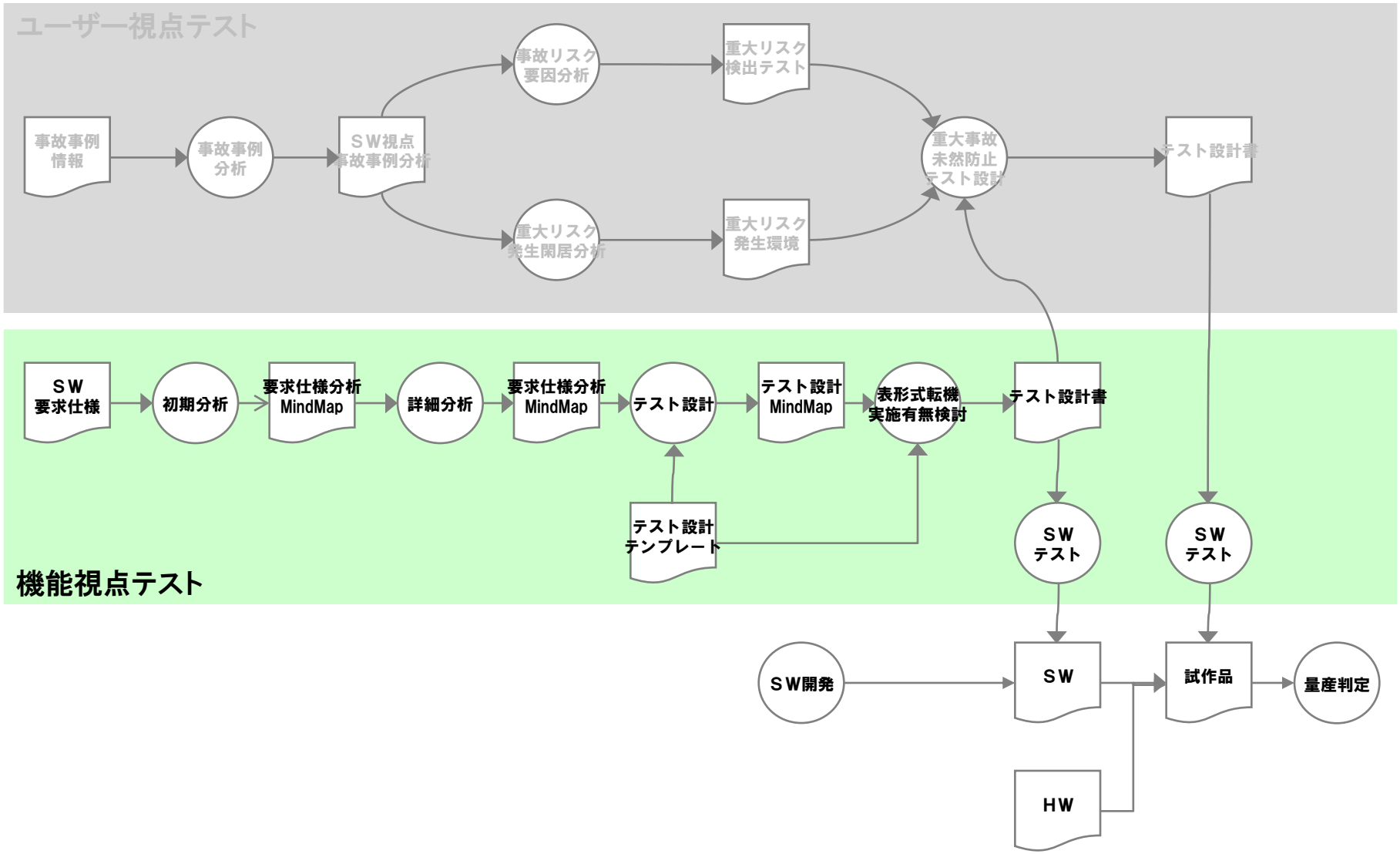
テスト設計プロセス

テスト設計プロセスフロー



テスト設計
（機能視点テスト）

テスト観点洗い出し（機能視点テスト）



[Step1] 要求仕様分析（初期分析）

初期分析として、話題沸騰ポット要求仕様全般をMind Mapに書き出す。分析対象を網羅かつ明確にし、”文章“により生じる曖昧さをできるだけ排除する。（粗いレベルの分析）

2．2 蓋	要求	pot-220	アイドルの状態で、蓋を閉じたら、水位を確認し、条件に合えば沸騰行為をする。
		理由	蓋を閉めるという行為で加熱（沸騰）の指示をしたい。
		説明	沸騰行為の詳細は、３章の「温度制御行為」に記載する。 蓋センサがonになって3sec経過するのを待つ理由は、注水やポットの移動の直後に、水面が波打っている状況が考えられるので、水面状態が安定する時間を想定したためである。
	<蓋「閉」を確認する>		
	□	pot-220-11	蓋センサが3sec以上onとなったら、蓋が閉じられたと判断する。
	<水量適性時の処理>		
	□	pot-220-21	蓋が閉じられ、水量が適正な場合、沸騰行為をする。 【説明】水量については、pot-280を参照。
	<水量異常時の処理>		
	□	pot-220-31	蓋が閉じられても、水量が異常な場合、状態はアイドルのままである。 【説明】水量については、pot-280を参照。
	要求	pot-221	
		理由	
		説明	
	□	pot-221-11	
	□	pot-221-12	
	□	pot-221-13	
2．3	要求	pot-230	

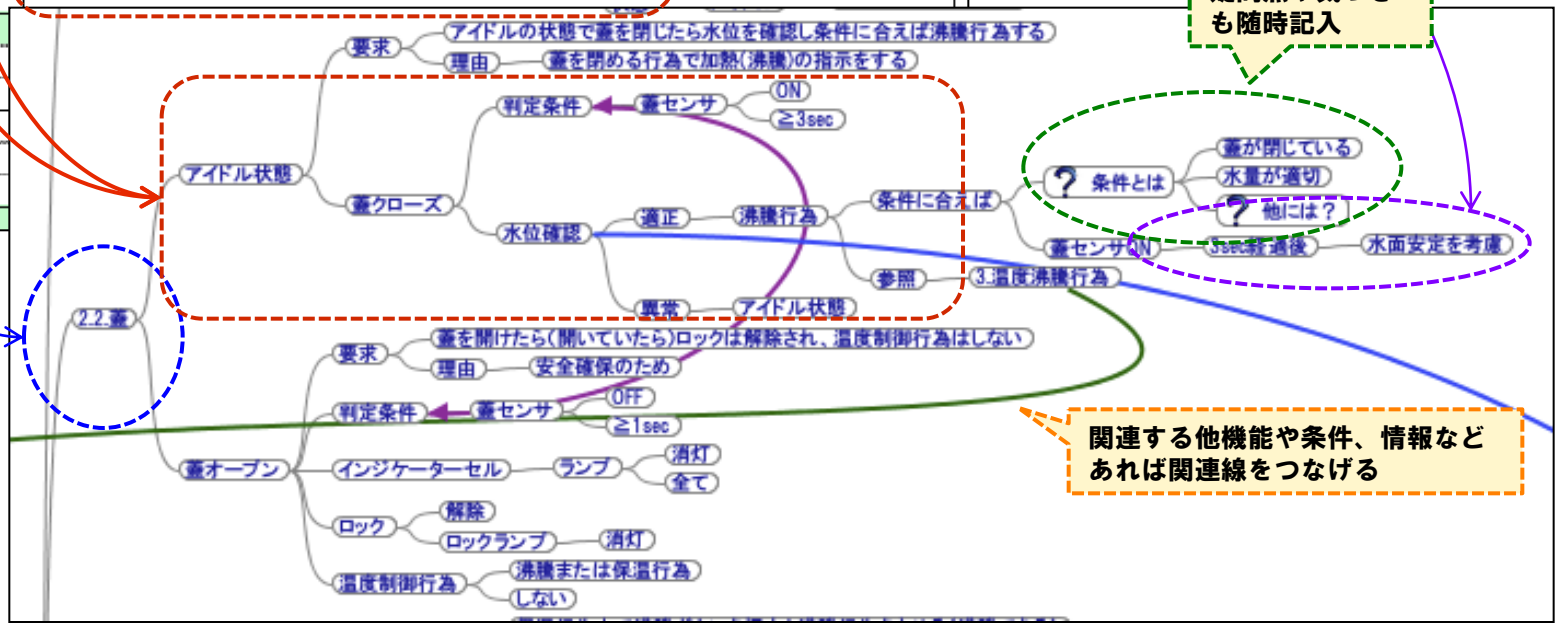
考慮すべき他の条件も追加

単語や短いセンテンスに分解してブランチに追加

疑問点や気づきも随時記入

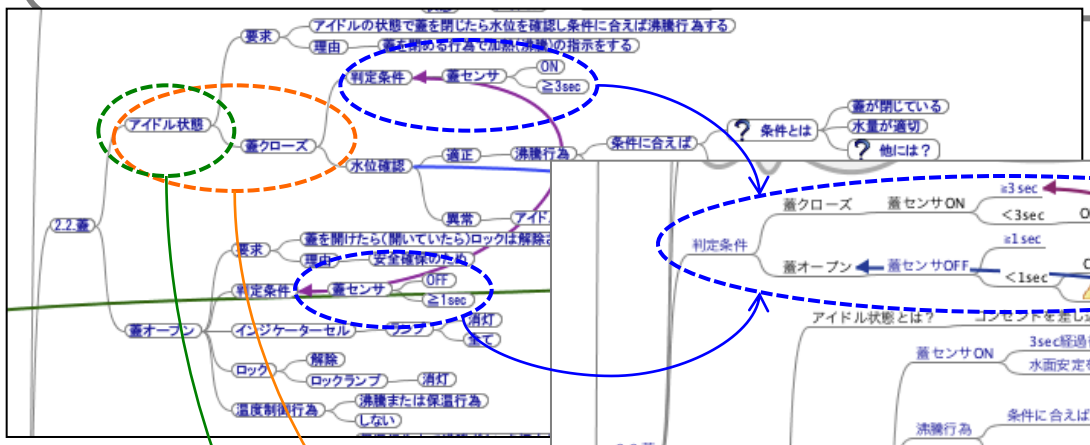
基本的に章立てと同じ構成

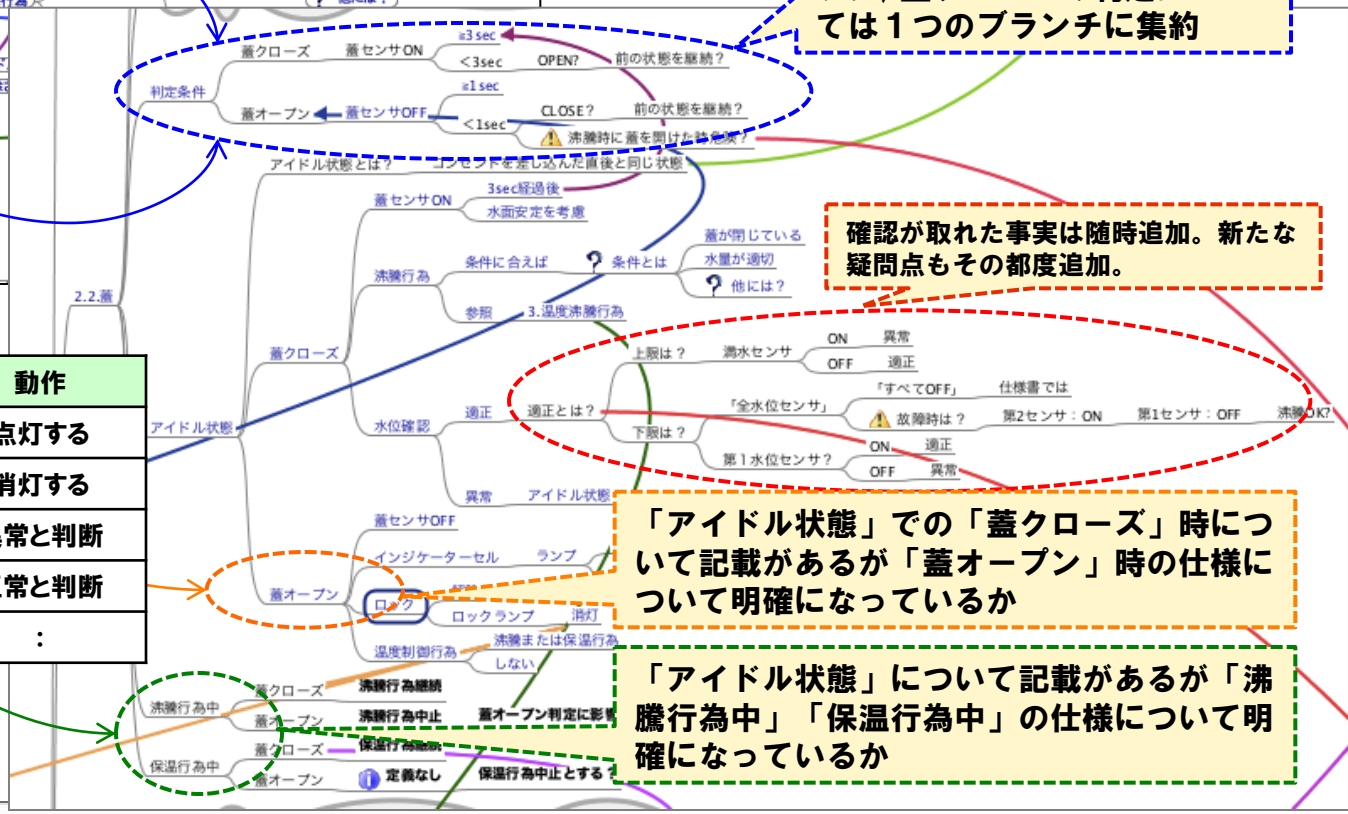
関連する他機能や条件、情報などあれば関連線をつなげる



[Step2] 要求仕様分析（詳細分析）

要求仕様から抽出できた条件、状態、動作、関連する他機能の仕様等に着目し、仕様のヌケモレや曖昧さを探す。明確になっていない条件や状態、動作がないか検討し、確認が取れた事実も随時書き込み、発散と集約を繰り返しながら、実現すべき機能を明確にしていく。（詳細レベルの分析）





条件
ON
OFF
蓋クローズ
蓋オープン
:

状態
アイドル状態
沸騰行為中
保温行為中
:

動作
点灯する
消灯する
異常と判断
正常と判断
:

複数箇所に点在している蓋オープン/蓋クローズの判定については１つのブランチに集約

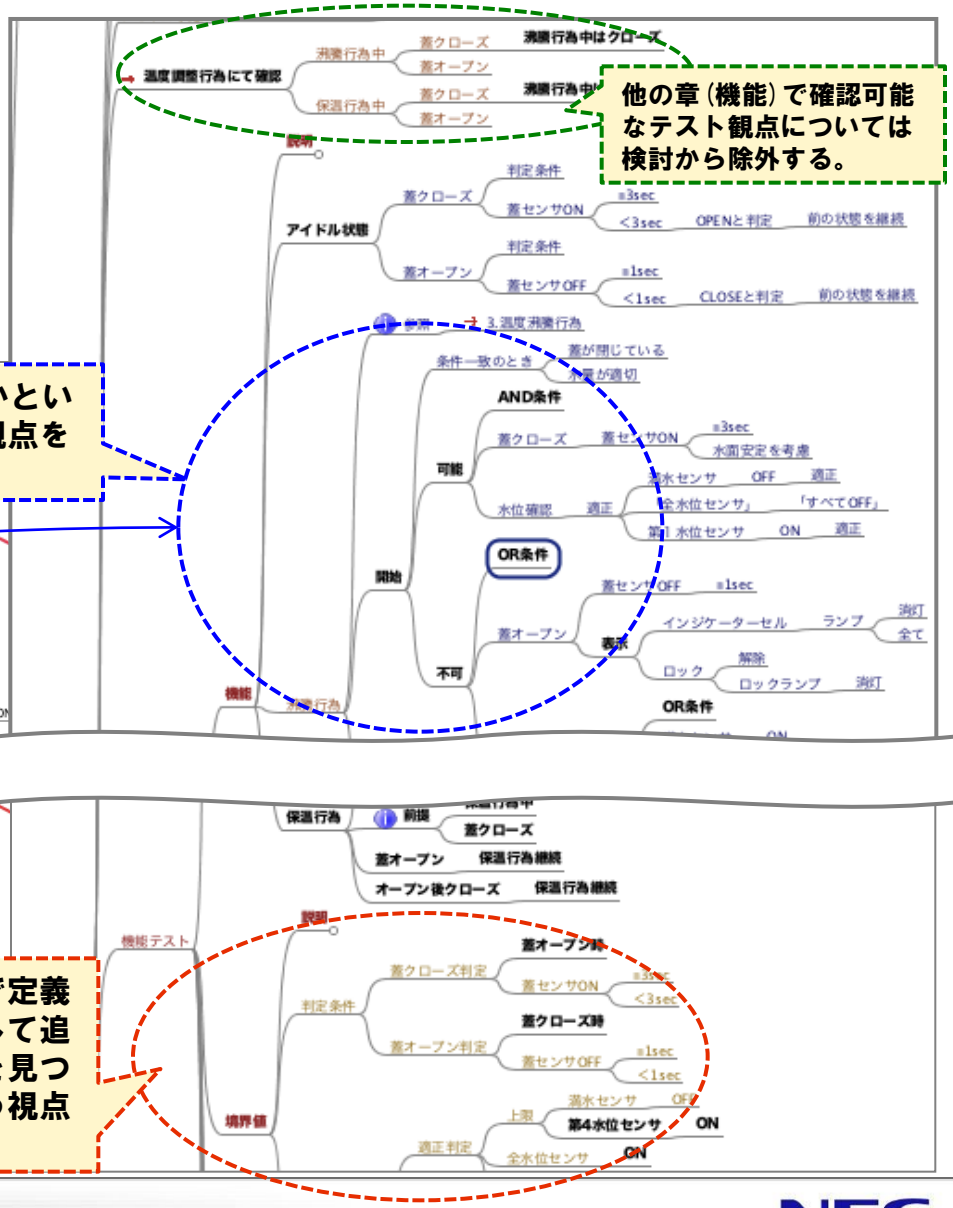
確認が取れた事実は随時追加。新たな疑問点もその都度追加。

「アイドル状態」での「蓋クローズ」時について記載があるが「蓋オープン」時の仕様について明確になっているか

「アイドル状態」について記載があるが「沸騰行為中」「保温行為中」の仕様について明確になっているか

[Step3] テスト設計（テスト観点追加）

明確化した機能に対して、何をどうテストするかという視点で整理し、仕様をチェックする。さらにテスト設計テンプレートからテスト観点を追加・検討し、テスト漏れがないことをチェックする。



テスト設計テンプレートとは

- テストのヌケモレの防止と、担当者によるバラツキの軽減を目的に、テスト技術コミュニティで作成した、テスト設計時に検討すべきテスト観点について整理したテンプレート。
- 関連する各文献を調査・分析。さらにＮＥＣグループ内の様々なドメイン(※)から参加しているテスト技術コミュニティメンバーの知見を導入。（※ ＳＩ、汎用ソフト、パッケージ、組み込み、など。）
- 機能テスト観点５種、非機能テスト観点１０種を標準として設定。
- テストレベルは実装技術に左右されにくい結合テストにスコープ。
- JaSST'09 Tokyo、JaSST'10 Tokyo にて事例発表。

テスト設計テンプレート

テスト設計テンプレート全体概要
テスト観点の網羅性向上のため「テンプレート」とし、機能・非機能とに分類して実装

テスト観点 (機能テスト観点)

テスト観点説明

テスト観点導出のヒントワード

実際のテスト観点

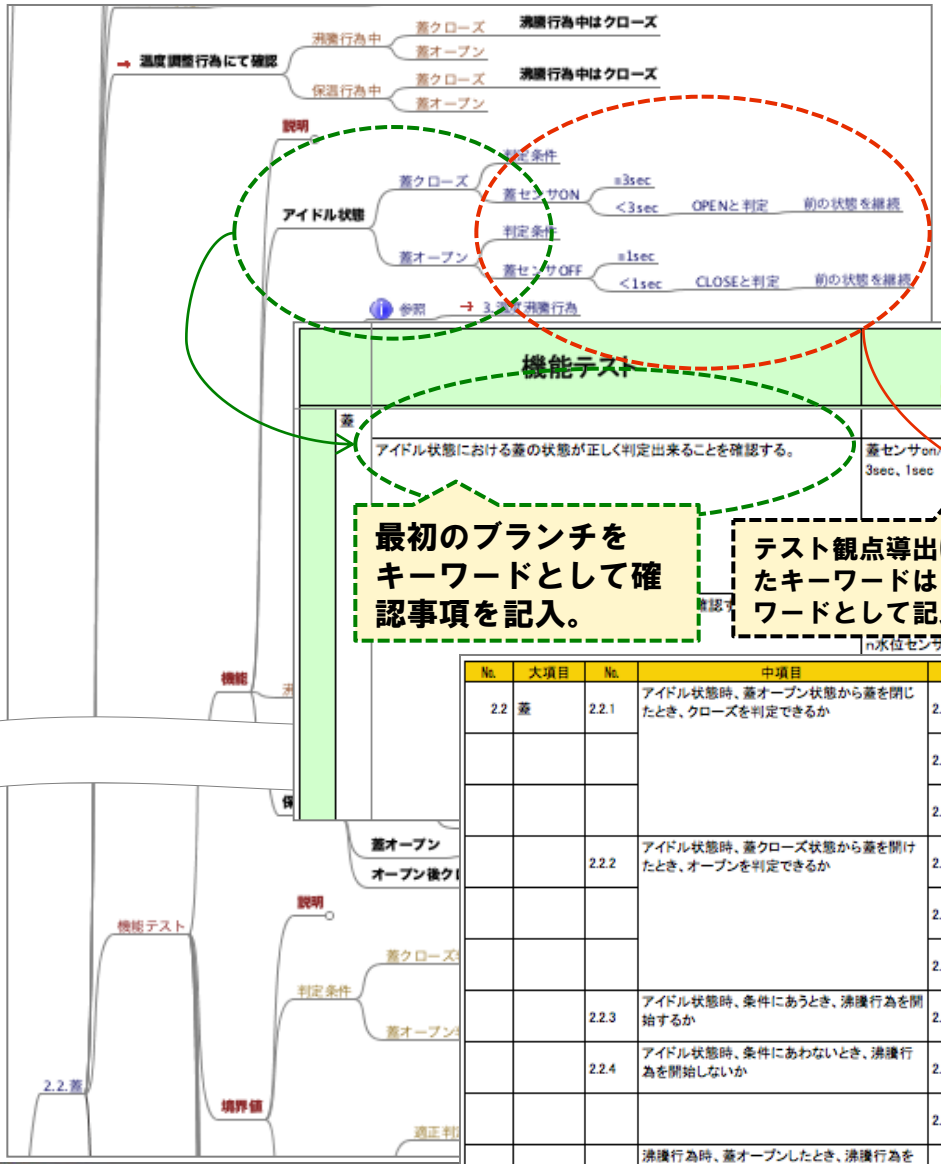
機能テスト	ヒントワード	実施の有無（○・×）	テスト観点
境界値 同値を意識した上で境界値を検討する。 値などに有効な範囲がある場合には、その上限・下限と、これをぎりぎり外れたものとを条件としてテストする。			
入力データに関する境界 入力されたデータが想定される範囲内の場合と範囲外の場合の処理が正しく行われていることを確認する。 ・数値の取りうる範囲の内外 ・集合の内外 ・データ長の範囲の内外	最大値、最小値 範囲内外 A<X<B、A≦X≦B A<X≦B		
ループの境界 各ループの境界（条件）が正しく処理できていることを確認する。 ・回数のループ ・条件のループ	0回ループ 無限ループ 再帰		
タイムアウト時間に関する境界			

非機能テスト観点カテゴリ整理

	品質特性（ISO9126）						Myersの14のシステムテスト・カテゴリ												
	機能性	信頼性	使用性	効率性	保守性	移植性	ボリューム	ストレス	効率	ストレージ	信頼性	構成	互換性	設置	回復	操作性	セキュリティ	サービス性	文書	手続き
操作性			○													○				
運用テスト					○														○	○
性能テスト				○				○												
信頼性テスト		○							○		○									
セキュリティテスト	○																○			
障害対応テスト		○																		
インストーラビリティテスト						○								○						
移植性テスト						○							○							
保守性テスト					○										○			○		
機器構成テスト		○				○	○			○		○								

テスト設計書・仕様書作成

MindMap上で行ったテスト設計結果を、テスト設計テンプレートに転記し、テスト設計書を作成する。テスト実施の有無についても改めて検討する。



機能テスト	ヒントワード	実施の有無 ○/×	テスト観点	補足	ID	安全性テスト
蓋						
アイドル状態における蓋の状態が正しく判定出来ることを確認する。	蓋センサon/off 3sec、1sec		・蓋を閉じる 蓋センサON時 ≧3sec：閉じられた <3sec：閉いたまま ・蓋を開ける 蓋センサOFF時 ≧1sec：開けられた <1sec：閉じたまま ・沸騰開始可能 蓋が閉状態で水位が適正(*1)であること *1(AND条件)：満水センサoff、全水位センサが全てoff、第1水位センサ		t-220-11 t-221-11	
	n水位センサ					

No.	大項目	No.	中項目	No.	小項目	確認日	確認者	結果	備考
2.2	蓋	2.2.1	アイドル状態時、蓋オープン状態から蓋を閉じたとき、クローズを判定できるか	2.2.1.1	蓋センサが3sec以上ONのとき、クローズと判定すること（常温の水が適量に入っている場合は沸騰行為になる。）				
				2.2.1.2	蓋センサON=3secのとき、クローズと判定すること（常温の水が適量に入っている場合は沸騰行為になる。）				
				2.2.1.3	蓋センサON=2secのとき、オープンと判定すること（常温の水が適量に入っている場合は沸騰行為になる。）				
		2.2.2	アイドル状態時、蓋クローズ状態から蓋を開けたとき、オープンを判定できるか	2.2.2.1	蓋センサが1sec以上OFFのとき、オープンと判定すること				
				2.2.2.2	蓋センサON=1secのとき、オープンと判定すること				
				2.2.2.3	蓋センサON=0.9secのとき、クローズと判定すること				
		2.2.3	アイドル状態時、条件にあうとき、沸騰行為を開始するか	2.2.3.1	以下の全ての条件が揃ったとき沸騰行為を開始するか ・水位が適正であること ・蓋がクローズしていること				沸騰行為の判定は「温度制御行為」参照 水位が適正かの判定は「水位メーター」参照
		2.2.4	アイドル状態時、条件にあわないとき、沸騰行為を開始しないか	2.2.4.1	水位異常時に沸騰行為を開始しないこと（蓋クローズ時）				
				2.2.4.2	蓋オープン時に沸騰行為を開始しないこと(水位適正時)				
		2.2.5	沸騰行為時、蓋オープンしたとき、沸騰行為を	2.2.5.1	蓋センサが1sec以上OFFのとき、オープンと判定し、沸騰行為を				

レビューにて、実施有無を判断し、○または×を記入。実施しない場合は、理由を備考欄に記入。

各機能における条件や設定内容をテスト観点として記入。

最初のブランチをキーワードとして確認事項を記入。

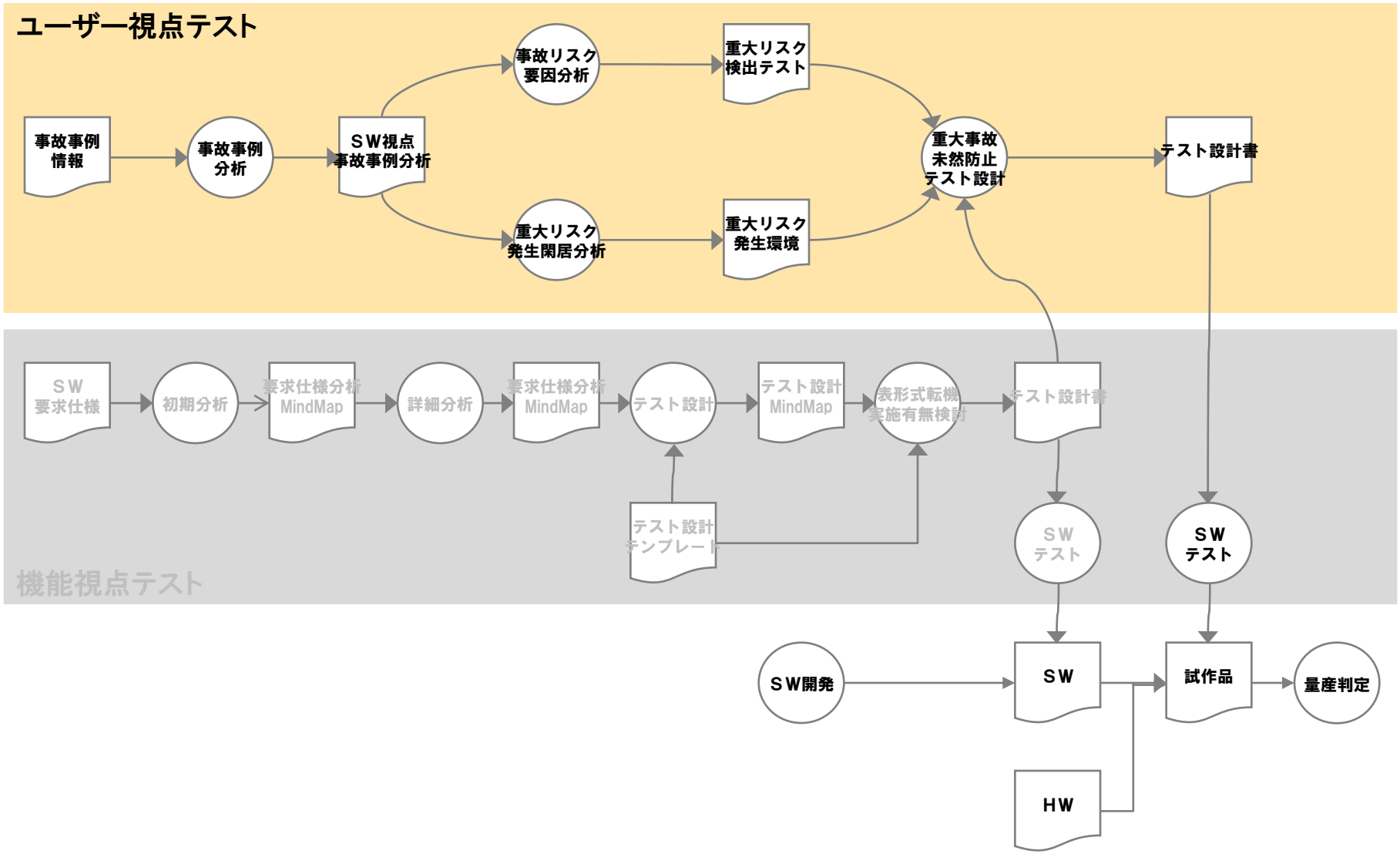
テスト観点導出に使用したキーワードはヒントワードとして記入。

要件番号を記入してトレーサビリティを確保。

テスト観点からテストケースを洗い出し、テスト仕様書に記載。

テスト設計
（ユーザー視点テスト）

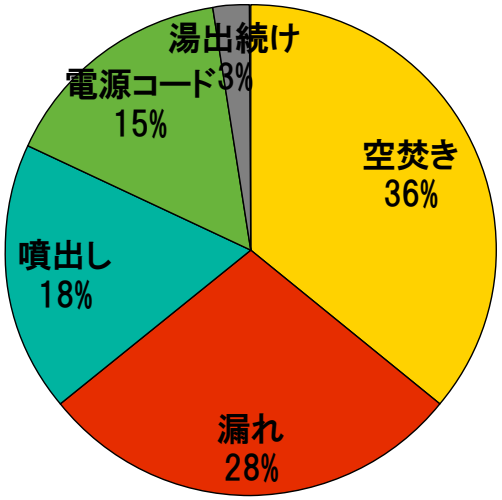
テスト観点洗い出し（ユーザー視点テスト）



事故事例分析に基づく利用者安全視点ついて

事故事例データベースを分析し、要因として何が多いのかを検討する。
要因については湯量減少による空焚き、水漏れや湯漏れ、湯の噴き出し、電源コードで分類。

事故状況グラフ（n＝１２０）



分析した事故情報データベースの概要

品名：電気ポット【電気湯沸器】で検索した１２０件のデータ
事故事例で報告のあったメーカー、輸入業者：２５社

通知者	件数
消費者センター	47
製造事業者	24
製品評価技術基盤機構	20
消費者	11
輸入事業者	6
国の行政機関	5
消防機関	5
経済産業省　重大製品事故(2007-2365)	1
経済産業省　重大製品事故(2009-2718)	1

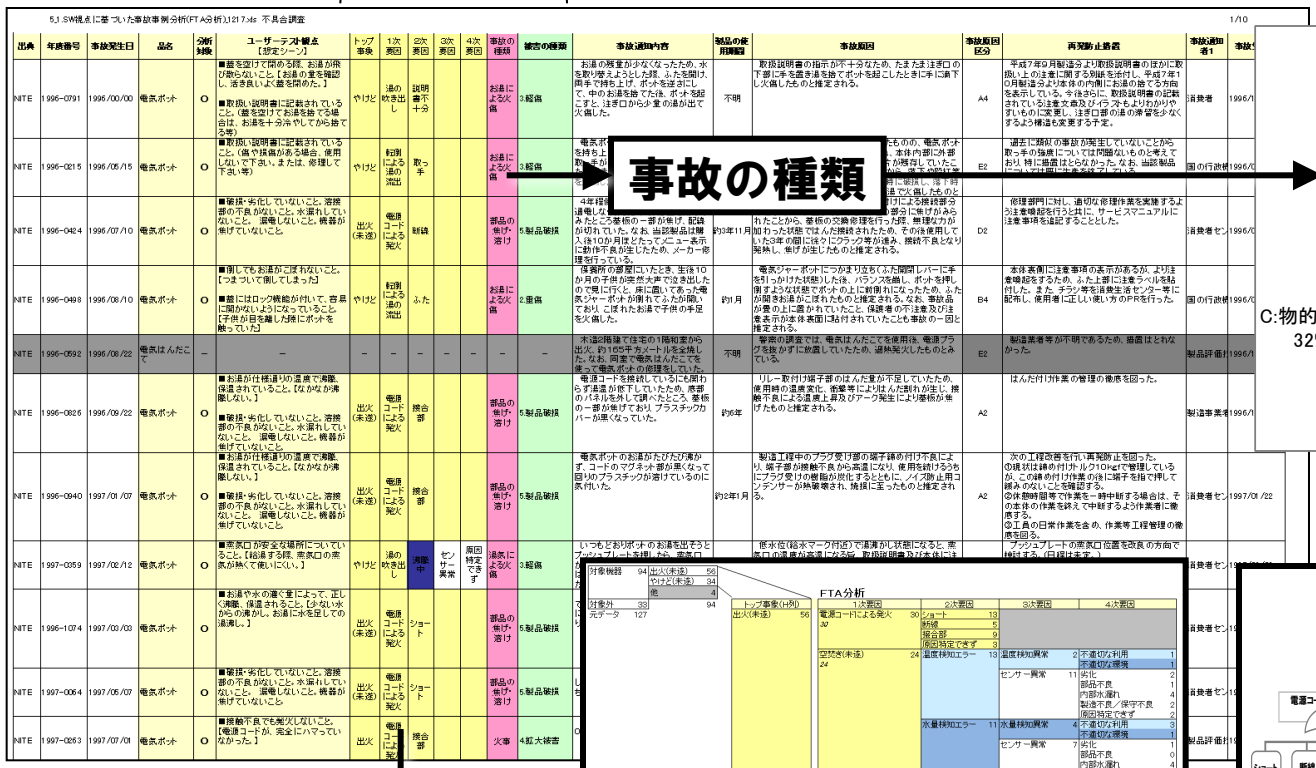
被害の種類	件数
4.拡大被害	47
5.製品破損	30
3.軽傷	26
2.重傷	9
6.被害なし	7
11.火災	1

この事故状況要因はハードウェア不良などが含まれるが、
発生要因がソフトウェアでないことをソフトウェアテストで確認できないかを検討。
安全性を確認するためのテストを検討した。

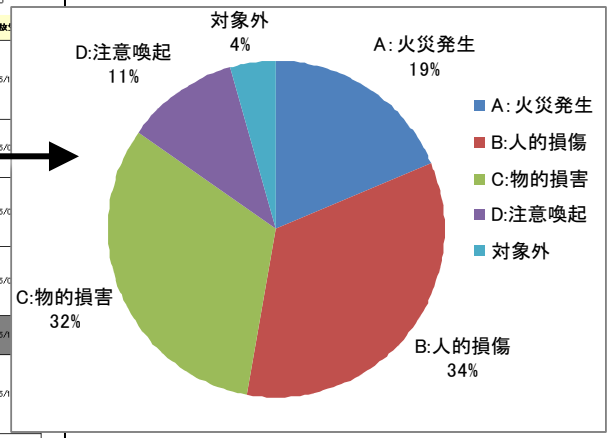
事故事例データベース分析

事故事例データベースに、分析用の項目を追加し、事故の部位や重篤差について分析できるようにした。

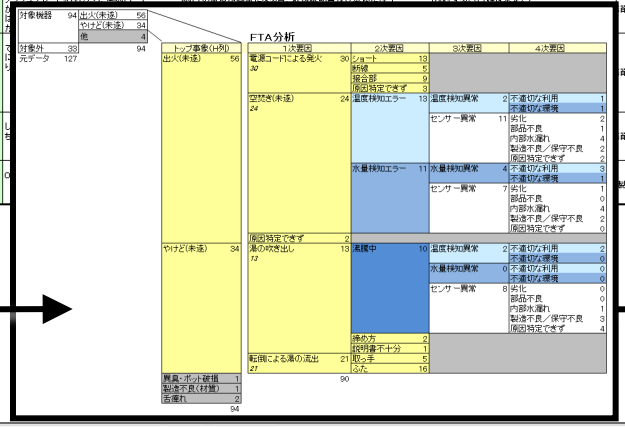
分析用に追加した項目

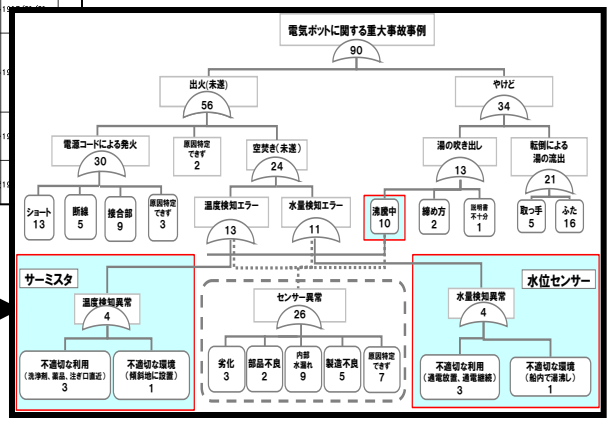


事故の種類



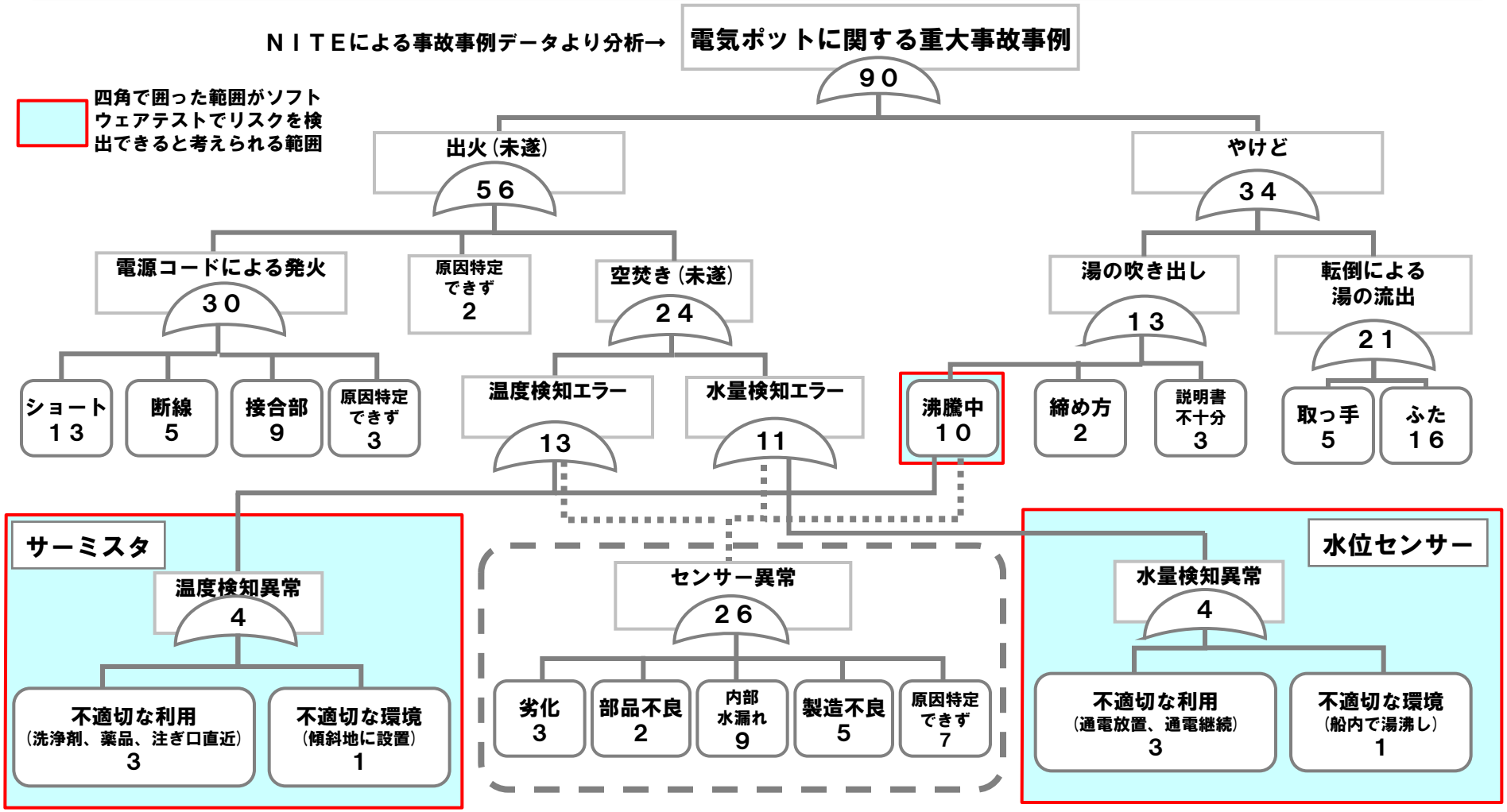
事故の部位から
ＦＴＡ分析





ソフトウェア視点に基づいた事故事例分析

電気ポットにおける事故事例から事故要因の分析を実施し、ソフトウェアテストで実施する範囲を抽出。



事故リスク要因分析（1）

事故リスクの分析の結果、温度検知異常と水量検知異常の
２つが重大な事故要因になっている。そのため、温度検知異常につながるサーミスタと水量検知異常の要因になる水位センサーに着目する。サーミスタの水温の検知状態でどのような結果になるか、また水位センサーの検知状態でどのような結果になるかを整理する。

サーミスタの水温検知が正常の場合と異常になる場合

項番	サーミスタの状況（Ｔ）			説明	結果
（Ｔ－１）	ポットに入っている水（湯）の温度	＞	サーミスタが検知した温度	【検知した水温が過小】 既に高温になっていても さらに沸騰しつづけるリスクが高まる	過熱
（Ｔ－２）		＜		【検知した水温が過大】 低温にも係わらず高温と感知するため いつまでも保温状態のまま	わかない
（Ｔ－３）		＝		【温度を正しく検知】	正常

水位センサーが水量を正しく検知した場合と異常になる場合

項番	水位センサーの状況(Ｗ)			説明	結果
（Ｗ－１）	ポットに入っている水量	＞	水位センサーが検知した水量	【検知した水量が過小】 満水を感知できずに沸騰し、 湯が噴出すリスクがある。	あふれる
（Ｗ－２）		＜		【検知した水量が過大】 少ない湯量を検知できないため、 空でも保温、沸騰する可能性がある。	過熱
（Ｗ－３）		＝		【水量を正しく検知】	正常

事故リスク要因分析（2）

サーミスタと水位センサーがそれぞれ状況が複合した場合を整理する。
比較的短時間に空焚きなどのリスクが顕在化するのは、サーミスタが温度を過小検知している場合であることがわかる。この場合、火傷や火災のリスクが高く、被害が甚大になる。

サーミスタの状況と水位センサーの状況の組合せによるリスク

		水位センサーの状況（W）			リスクの顕在化
		（W－１）あふれる	（W－２）過熱	（W－３）正常	
サーミスタの状況（T）	T－（１）過熱	沸騰した湯の吹き出し	空焚きのリスクが大きい	空焚きのリスクがある	短時間で顕在化
	T－（２）わかない	いつまでも保温状態	徐々に水量が減り、空焚きになる	いつまでも保温状態	顕在化に時間を要する
	T－（３）正常	満水の際吹き出す	徐々に水量が減り、空焚きになる	（正常）	顕在化に時間を要する

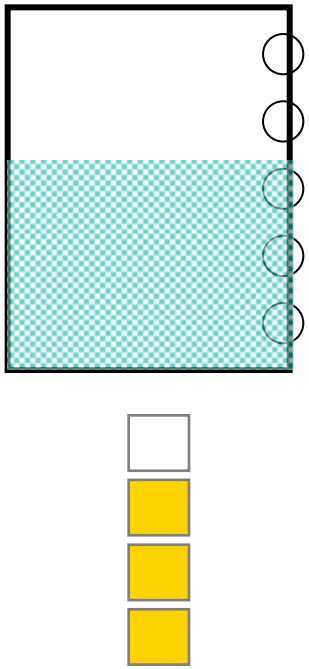
重大リスク発生環境

電気ポットが使用される環境によって、サーミスタや水位センサーが誤作動する可能性がある。
これらの可能性を事故事例から分析する。

利用環境・発生環境	説明	影響を受けるセンサー	
		サーミスタ	水位センサー
洗浄剤	洗浄剤は発泡性のものがあり 保温状態や沸騰状態で使わないようにマニュアル等に記載はされていることが多い。	●	●
異物 （化学薬品など）	故意に入れる場合があるが、重大事故につながる可能性は大きい。	●	●
気圧変化	高度が増して気圧が減少すると地表よりも低い温度で沸騰する	●	ー
ゆれる場所での使用	船の中など設置場所が安定しない場合は 水量検知が異常になる	●	●
傾いた場所での使用	仕様では、水位センサーは片側についているので、傾いた場所では水量を過小もしくは過大に検知する可能性がある。	ー	●

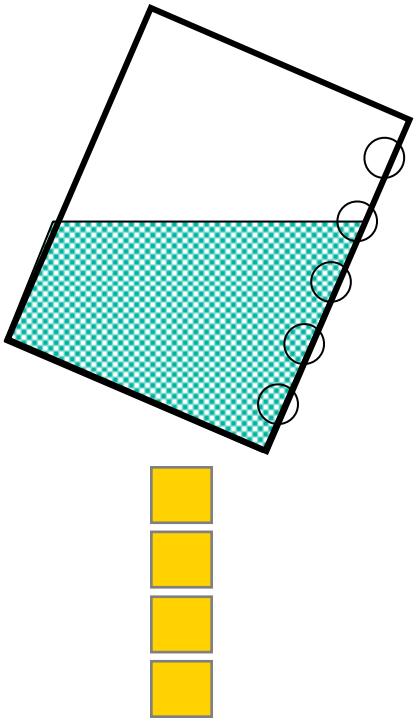
傾いた場所においた場合の例

水平な場所の場合



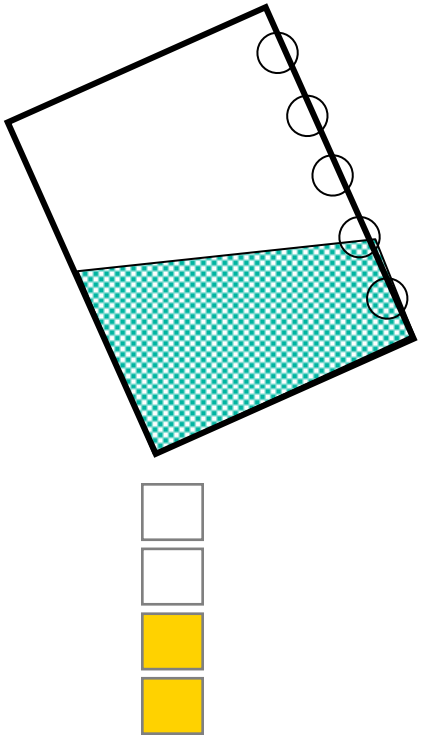
インジケータ表示

水位センサーがある方向に傾いていた場合



インジケータ表示

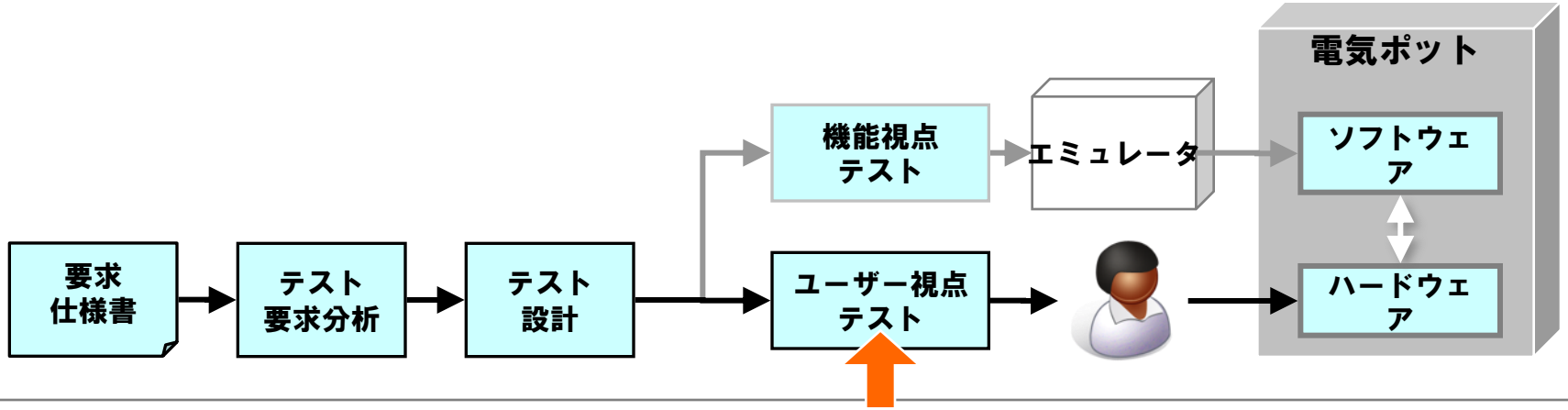
水位センサーがある方向とは反対に傾いていた場合

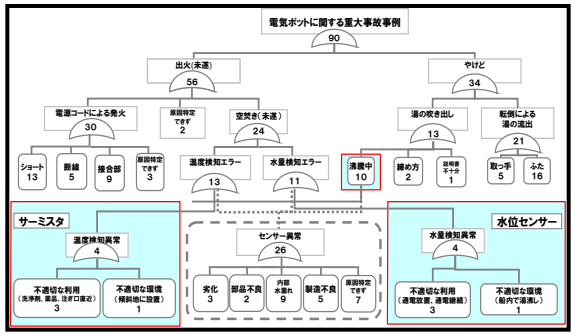


インジケータ表示

テストケース洗い出し

事故リスク要因と重大リスク発生環境をもとに、重大な事故を未然に防止するためのテストケースを洗い出した。





		水位センサーの状況(W)			リスクの顕在化
		(W-1) あふれる	(W-2) 過熱	(W-3) 正常	
サーミスタの状況(T)	(T-1) 過熱	沸騰した湯の吹き出し	空焚きのリスクが大きい	空焚きのリスクがある	短時間で顕在化
	(T-2) 湧かない	いつまでも保温状態	徐々に水量が減り、空焚きになる	いつまでも保温状態	顕在化に時間を要する
	(T-3) 正常	満水の際吹き出す	徐々に水量が減り、空焚きになる	正常	顕在化に時間を要する

利用環境・発生環境	説明	影響を受けるセンサー	
		サーミスタ	水位センサー
洗浄剤	洗浄剤は発泡性のものがあり、保温状態や沸騰状態で使わないようにマニュアルなどに記載されていることが多い。	●	●
異物(化学薬品など)	故意に入れる場合があるが、重大事故につながる可能性は大きい。	●	●
気圧変化	高度が増して気圧が減少すると地表よりも低い温度で沸騰する	●	–
ゆれる場所での使用	船の中など設置場所が安定しない場合は水温検知が異常になる	●	●
傾いた場所での使用	仕様では、水位センサーは片側についているので、傾いた場所では水量を過小、もしくは過大に検知する可能性がある	-	●

ユーザー視点テストで考慮すべき事項

フィードバック

要求仕様に関するフィードバック

条件や設定に関する記載事項をみると様々な記載方法が混在しており、これらの記載方法が要求分析の際にヌケモレや誤解を招くリスクがある。これらの記載方法をルール化しておくことで要件分析の精度も向上できる。

条件	条件になったとき
	条件に合えば
	○○たら、
	○○となったら、
	○○と、
	○○を確認し、
	○○になったら、
	終わったら、
	終えたら、
	○○後は、
	○○した後、
	○○したら、
	○○によって
	度に
	時に
	○○の中に
	タイムアップしたら
	○○間隔で
複合条件	○○から○○まで
	いずれかの時、
	全てを満足する場合、
	○○で
	○○られ、

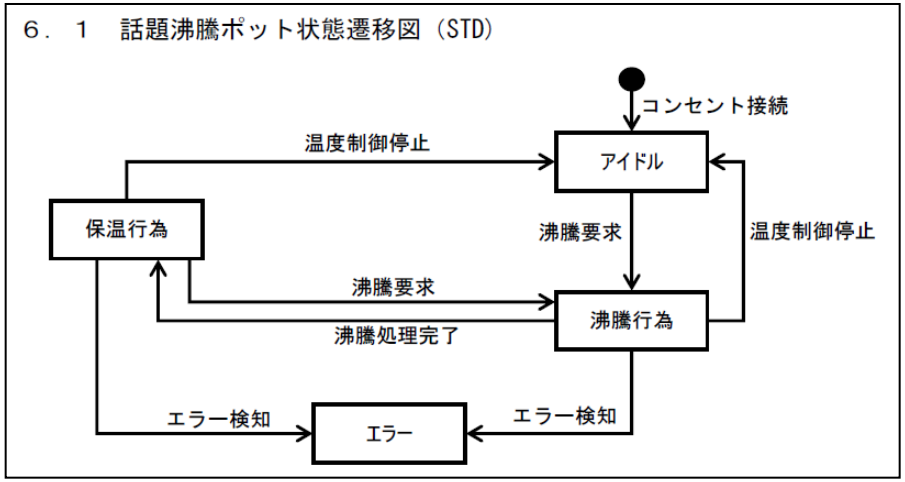
否定条件	いない場合は、
	1つでも満たしている場合は、○○しない。
	でなければ
	しても
	でも
	かかわらず、
否定 複合条件	○○ても
	さず、
	○○も○○も

設定	○○にする
	判断する
	○○する
	○○できる
複合設定	○○され、
	○○し、
	○○した後、
	それぞれ○○する
	し終え、
設定しない	○○しなくなる
	中止する
	やめる

ソフトウェア開発チームへのフィードバック

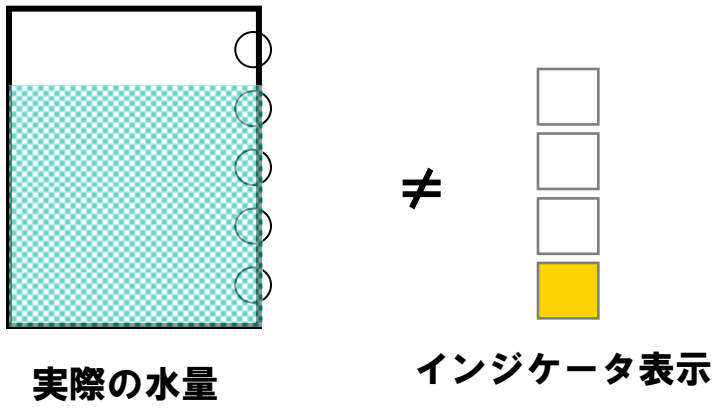
電気ポットを利用する上で、ユーザーにとって製品リスクについて２点取り上げる
（１）電源投入後の沸騰モード
（２）インジケータランプの仕様

（１）電源投入後の沸騰モード



コンセント接続後アイドル状態を経て沸騰行為に遷移する仕様
しかし、保温モードによっては、沸騰行為を中断してもよいはずではないかと考える。また、
「ミルクモード」のお湯を使えるようになるまでは相当の時間を要する

（２）インジケータランプの仕様



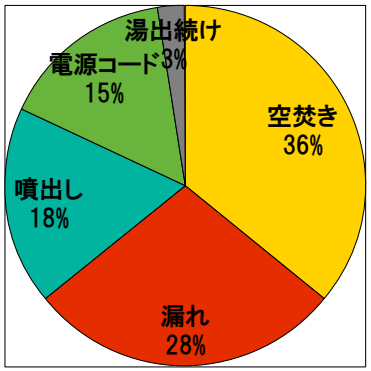
満水センサーは別な機能としての位置づけになっているが、水位センサーは、ひとつが故障してポット全体への影響を回避する。そのため、水位は正確に把握した結果は利用者にも正しく通知すべきと考える。

ハードウェア開発チームへのフィードバック

事故事例分析に基づき、安全上のリスク軽減のため、下記２点の仕様への反映を提案する。
（１）電源コード
（２）圧力センサー

（１）電源コード

電源コードの要因で事故（火災）が発生するケースが１７％を占めている。
電源コードに関しては電気製品には必ず懸案事項となるものなので、下記のような仕様の追加を提案する。



提案１：
電源コードのコンセント部、本体接合部に電圧測定装置を入れ、ショートを防止する。

提案２：
本体と電源コードを磁石ではなく粘着性のものに変更する。
（電源コード接続部の磁石に金属異物がついてショートした事例に基づく）

（２）圧力センサー

吹き出し事故の中には、異物（洗浄剤）などのために過圧されるリスクがあった。
取り扱い説明書等に注意事項が書かれているが、あくまで利用者の注意によるものである。
また高度では気圧低下により沸点が下がることも考慮する。

提案１：
圧力センサーを装備し、過圧状況ではすべての電源を遮断するようにする。

提案２：
電気ポットが製品仕様を超えた気圧環境で使用された場合は、電源を遮断するようにする。

おわりに

われわれは、利用者の安全をソフトウェアの立場でテストすることを検討してきた。
これはどれほど多くのテストをしたとしても利用者が被害を受ける事態があってはならないと考えたためである。

事故事例データベースを見てみると様々な製品での事故が報告されているが、直接ソフトウェア起因である報告は少ない。
しかし、事故状況から分析するとソフトウェアの不具合によって発生しうる可能性もゼロではないことがわかる。

事故事例では、子供の大やけどや火災による人命が失われるものも含まれている。
こうした、事例に基づいてテストを検討することは、設計時の考慮漏れを防ぐ意味でも重要と考える。