社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
KBSE2011-61 (2012-01)

要求表に基づくディペンダビリティ情報作成方法

猿渡 卓也[†, †2] 山本 修一郎[‡]

†名古屋大学大学院情報科学研究科〒464-8601 愛知県名古屋市千種区不老町

‡名古屋大学情報連携統括本部〒464-8601 愛知県名古屋市千種区不老町

†2 株式会社NTTデータ 〒135-8671 東京都江東区豊洲 3-3-9

E-mail: †saruwatarit@nttdata.co.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

あらまし 要求を①識別子，②要求名，③説明，④理由などの表形式の表現（要求表）を用いて文書化する方法が，システム開発では広く用いられている．しかし，機能数が数百以上になる実用規模のシステムで要求表を使用すると，理由が機能ごとに断片的に記述されるため，要求表の中のディペンダビリティを確認することが煩雑になり困難になる．そこで，要求表を分析しグラフ構造に変換して提示することによりディペンダビリティ情報を分かりやすく提示する方法を提案する．

キーワード 要求表，Assurance Case，GSN，ディペンダビリティ

A dependability information creation method based on a requirement table

Takuya SARUWATARI[†, †2] Shuichiro YAMAMOTO[‡]

† Graduate School of Information Science Nagoya University Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan

‡ Strategy Office, Information and Communications Headquarters Nagoya University
Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan

†2 NTT DATA CORPORATION 3-3-9, Koto-Ku, Tokyo, 135-8671 Japan

E-mail: †saruwatarit@nttdata.co.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

Abstract Requirements document in tabular form is widely used in systems development. However, if the number of functions used in a table becomes hundreds or more, it will become difficult to check. In this paper, a method to develop GSN graphs based on requirements tables is proposed.

Keyword Requirements table, Assurance Case, GSN, dependability

1. はじめに

情報システムの用途が多様化し対象が複雑になるにつれ，情報システムのDependabilityを確保することが難しくなってきている．例えば，複数の情報システムを連携させて利用する場面を考えると，個々の情報システムに関するDependabilityの確保は検討されていても，それら複数の情報システムを連携して使用する時の検討は行われていないことも多い[1].

一般に情報システムのDependabilityを確保することは，情報システムを安心して利用する上で重要な課題となる．なぜなら，Dependabilityを確保できていないことが，後に安全上の問題を引き起こす可能性を持つからである．特に，組み込み系システムではDependabilityに関する欠陥の影響が，現実世界の中で物理的に影響を及ぼす可能性を持つ．例えば，電気ポットにおけるヒータ機能の制御ミス（空焚き等）による火災発生などである．このように，Dependabilityの確保は重要な課題となっている．

近年，この状況を受けてAssurance Case(Safety Case)の利用が進められてきており，実問題に対する適用事例の報告なども増加している[1][2][3][4][5]．一般的にAssurance Caseの構築には，目的を構造的に整理できるGSN(Goal Structuring Notation)が利用されている．GSNは，一般的なゴール指向要求分析で使うNFRやKAOSのような階層型のゴールグラフの記法であるが，「ゴール分割時のStrategy（ゴール分割戦略）の定義が可能」，「最下位のゴールに対するSolutionの付与が可能」，「GoalやStrategyへの付加情報（Justification, Assumption, Model）の付与が可能」の3点が特徴となっている．Assurance CaseでGSNを利用する場合は，SolutionをEvidenceと置き換える．すなわち，Assurance Caseに含まれるGoalは，Evidenceによって保障されるとする考え方になる．また，Assurance Caseは，上

流工程のみで作り上げるのはなく情報システムのライフサイクル全体を通して作り上げていくものとなる．例えば，Evidence には試験工程における試験結果を充当することが行われている．GSN で Assurance Case を構築することにより，情報システムのライフサイクル全般で Dependability に関する情報を構造化して把握・理解することができ，Dependability の検討不足の軽減が期待できる．

一方，現状の情報システム開発では，情報システム構築の上流工程でまとめられる要求に Dependability に関するものも含まれている．例えば，組み込み系システムの開発では，USDM（Universal Specification Description Manner）[6]という表形式の記法を利用した要求仕様記述が広く用いられており，その中に Dependability に関する要求も含まれている．これら要求表は Dependability に関する要求以外に，他の要求も多く含んでいる．そのため，Dependability に関する要求が要求表の中に散在しており，それらを構造的に把握するのが難しい状態となっている．そのため，情報システムの Dependability に関する情報に抜け漏れ等が起こる危険性がある．

本稿では，このような状況に対処するため，要求表に散在する Dependability に関する情報を抽出し Assurance Case を構築する手法を提案する．提案手法を使うことにより，要求表から Assurance Case を得ることができる．ただし，本稿で提案する手法で得られるのは，要求表に含まれる情報のみを利用した Assurance Case となる．上述の通り要求表には Dependability に関する情報の抜け漏れ等が存在する可能性がある．そこで，本稿で提案する手法で Assurance Case を構築後，情報システム構築を通して，作成した Assurance Case を完成させ管理していく必要がある．

2. 提案手法

提案手法は 3 つの手順からなる“提案プロセス”と，手順で使用する “要求分析シート”，“リファレンスモデル” の 2 つのツールで構成されている．以下の小節で，“要求分析シート”，“リファレンスモデル”，“提案プロセス” について説明する．

2.1. 要求分析シート

一般的に要求表の要求文は自然文で書かれており，様々な表現が使われている．そのため，要求文をそのまま理解しようとすると，受け取り手により理解に差が生じる可能性がある．その差を減少させるため，後の節で説明する提案プロセスでは，要求文を「要求を実現する主体(主体)」,「要求が求める変更操作(操作)」,「要求が求める変更操作の対象（対象)」,「要求が依存している環境(環境)」,「要求が充足された状態(結果)」の 5 つの要素に分割する（図 1)．要求分析シートは，分割した要求文を整理してまとめるための表である．

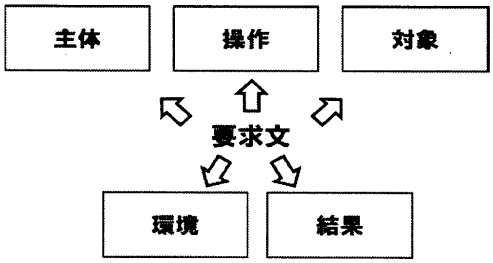

図 1 要求文の分割

表 1 に要求分析シートの例を示す．要求分析シートでは，1 行につき 1 つの要求について整理する．要求文の中には，複数の要求が含まれている可能性がある．そのような場合，要求分析シートでは，複数の要求として複数行に整理する．要求分析シートの 1 行は，GSN グラフの 1 つの Goal に対応する．

表 1 要求分析シートの例

主体	環境	操作	対象	結果

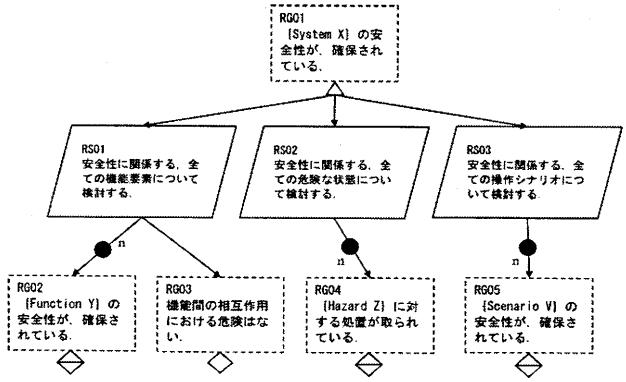

図 2 リファレンスモデル

2.2. リファレンスモデル

提案プロセスでは，Assurance Case 構築のためリファレンスモデルを利用する．[2]では，Safety Case のパターンを作成するための記法が，示されている．また，Safety Case の木構造のグラフの中で，最上位のレベルで利用するパターンの例が 2 つ示されている．本稿では，そこで示されている 2 つのパターンを組み合わせ，新規に 1 つの Strategy と 1 つの Goal を追加してリファレンスモデルを定義した（図 2)．点線で囲った Goal は，Assurance Case 構築時に具体的な Goal で置き換える必要があるものである．このリファレンスモデルの最上位の Goal は，対象となる情報システムの安全性の確保である．その最上位の Goal に対して機能要素（プ

ロダクト），危険な状態（環境），操作シナリオ（プロセス）の3つのStrategyにより検討するとしている．

2.3. 提案プロセス

提案プロセスは，順番に実施されることが想定されている三つの手順から構成される（図 3）．

図 3 提案プロセス

提案プロセスの各手順を，以下に説明する．

1. 【手順 1】安全性要求の抽出
   まず，対象としている要求表から，安全性に関する要求文を抽出する．次に，抽出した要求文を分析して“主体”，“環境”，“操作”，“対象”，“結果”に分割し，要求分析シートを利用して整理する．
2. 【手順 2】Goal の作成
   要求分析シートの情報から Assurance Case で使用する Goal を作成する．Goal 中のゴール文は，要求分析シートの“主体”，“対象”，“操作”に分割された要素を使って作成する．また，“環境”に分割された要素は，Goal に付与される Context とする．（Context は，GSN の拡張書式である[2]．本稿の手法では，Goal が依存する環境を表現するため Context の書式を利用している）
3. 【手順 3】Assurance Case の構築
   下記の 3 つのポイントをふまえ，リファレンスモデル（図 2）と，（手順 2）で作成された Goal を使って Assurance Case を構築する．
   - ポイント①
     Goal が，元の要求表で上位要求と下位要求の関係にある場合，Assurance Case でもその関係を導入する．
   - ポイント②
     Goal が安全性に関するものでなかった場合，Assurance Case の対象から外す．
   - ポイント③
     下位 Goal が充足されても上位 Goal の充足が十分説明できない場合，すなわち上位 Goal と下位 Goal の間に論理の飛躍があることがわかった場合，適当な Goal を追加して論理の飛躍をなくす．

以上の提案プロセスを実行することにより，要求表に含まれている Dependability に関する情報を抽出し，Assurance Case を構築することができる．ただし，要求表に含まれる情報のみから構築した Assurance Case は，Dependability に関する情報が不足していることが考えられる．例えば，Assurance Case の Evidence に関する情報は，情報システム構築のテスト工程の結果が利用されるなど，要求表に含まれていないことも多い．また，構造的な整理ができていない要求表では Goal そのものの抜け漏れが存在する可能性が高い．Assurance Case を完成させるために，提案プロセスを実施後に，一般的な Assurance Case 構築手法による検討構築が必要となる．

3. 手法の適用

情報システム開発の現場では要求は多様な様式の文書として表現されており，表形式による要求の表現も一般的に行われている．要求を表形式にすることの利点は，要求を計測可能な粒として扱えることができる点にある．特に，日本の組み込み系システムの開発では，表形式を用いた USDM[6]による要求記述が多く見られる．そこで，本稿では USDM で書かれた要求仕様書に対して，提案手法の適用を試みた．具体的には，USDM で書かれた要求表から Dependability に関する情報を抽出し，Assurance Case の構築を試みた．

表 2 USMD で書かれた要求表

ID	区分	要求
R1	要求	蓋を開けたら（開いていたら），ロックは解除され，温度制御行為はしない．
	理由	安全確保のため．
R2	要求	給湯に対するロック／ロック解除機能を付ける．
	理由	幼児などが給湯目的以外で誤って給湯ボタンを押してもお湯がでないようにするため．
R3	要求	給湯ボタンを押すことによって給湯口から給湯する．
	理由	ポットを持ち上げることなく，また給湯ボタンを無意識に押して期待していないタイミングでお湯が出て怪我（やけど）しないように，給湯したいから．
R4	要求	想定外の高温状態になった場合はエラーを検知し，ヒータ機能を停止する．
	理由	過熱による火災等の危険を回避するため．

3.1. USDM の要求仕様書

手法の適用対象には，インターネット上で公開されている“話題沸騰ポット”[7]の要求仕様書を利用した．この要求仕様書は，電子ポットを題材にしており，組

込みシステムの分析・設計のために作成されたものであり USDM を使って記述されている．本稿では，できるだけ曖昧さをなくした仕様書の例として作成されている“話題沸騰ポット要求仕様書（GOMA-1015 型）第 7 版”を利用した．この仕様書には 18 個の上位要求と 57 個の下位要求が含まれている．

USDM では，要求に対して，その理由を記述することができる．“要求の理由”は，その要求の上位要求なので，“要求の理由”もまた要求であると考えることができる．そこで，今回の手順適用では，安全性に関係すると考えられる上位要求の“要求文”と“理由文”を，要求の抽出対象として利用した．実際に抽出し利用した情報を表 2 に示す．

3.2. 手法の適用

表 2 で示される要求表の要求文と理由文に対して，本稿で提案した手法を適用し，Assurance Case の構築を試みた．以下に手法適用の過程を，手法のプロセスに含まれる 3 つの手順に分けて説明する．

3.2.1. 手順 1

手順 1 では，表 2 に示した R1 から R4 までの要求文と理由文を，要求分析シートを使って整理した．要求分析シートを使って分析した例として，R1 の要求文を分析する様子を図 4 に示す．この図の「要求文の整理」に示している項目が手順 1 の結果として要求分析シートに整理される．R1 の要求文は，詳細に分析すると要求文に二つの要求が含まれていることがわかった．そこで，R1 は二つの要求に分割されている．図は，R1 の要求文を二つの要求に分けて整理する様子を表している．図 4 では，手順 2 で作成する Goal 文も「ゴール」の欄に示している．

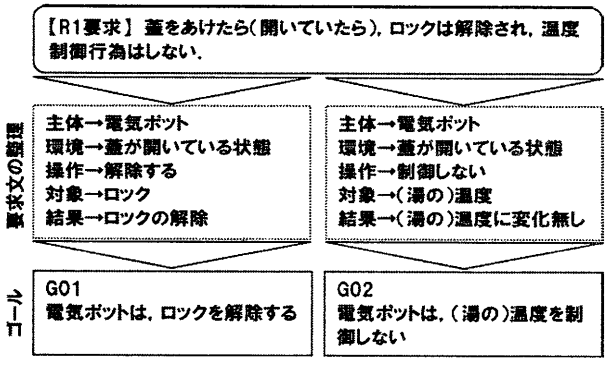

図 4 要求文の分析例

3.2.2. 手順 2

手順 1 で作られた要求分析シートの情報を利用して，Assurance Case の Goal（Goal 文）を作成した．作成した 11 個の Goal を一覧化したものを表 3 に示す．この段階では，まだ安全性とは無関係の Goal が含まれている．また，作成された Goal には，G07 と G08 のように，同じ内容「“電気ポットは，湯を出す”」のものが存在することがある．

表 3 作成された Goal 要素一覧

ID	Goal
G01	電気ポットは，ロックを解除する
G02	電気ポットは，(湯の) 温度を制御しない
G03	電気ポットメーカーは，電気ポットの安全を確保する
G04	電気ポットは，給湯をロックする
G05	電気ポットは，給湯のロックを解除する
G06	電気ポットは，湯を出さない
G07	電気ポットは，湯を出す
G08	電気ポットは，湯を出す
G09	ユーザーは，やけどをしない
G10	電気ポットは，ヒータ機能を停止する
G11	電気ポットは，火災等の危険を回避する

作成した Goal と，要求分析シートの環境から作成される Context を組み合わせて図化した．図 5 に作成された Goal と Context を図化したものの一部を示す．この図の 3 つ目と 4 つ目の Goal と Context は，Goal としては同じ内容だが，Context が異なっている Goal の例である．Context として，G07 には「給湯ボタンが押下された状態」が付与され，G08 には「ポットが持ち上げられていない状態」が付与されている．

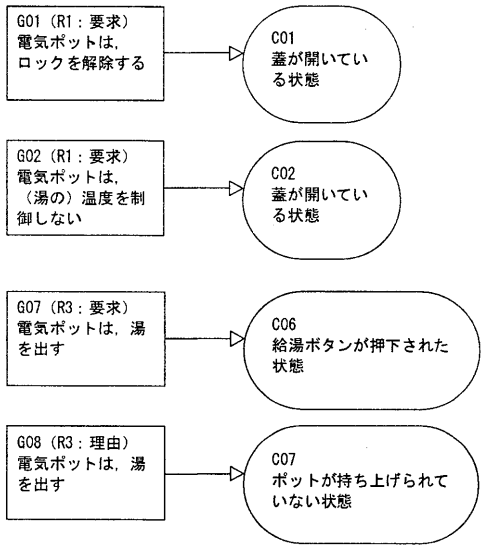

図 5 Goal と Context

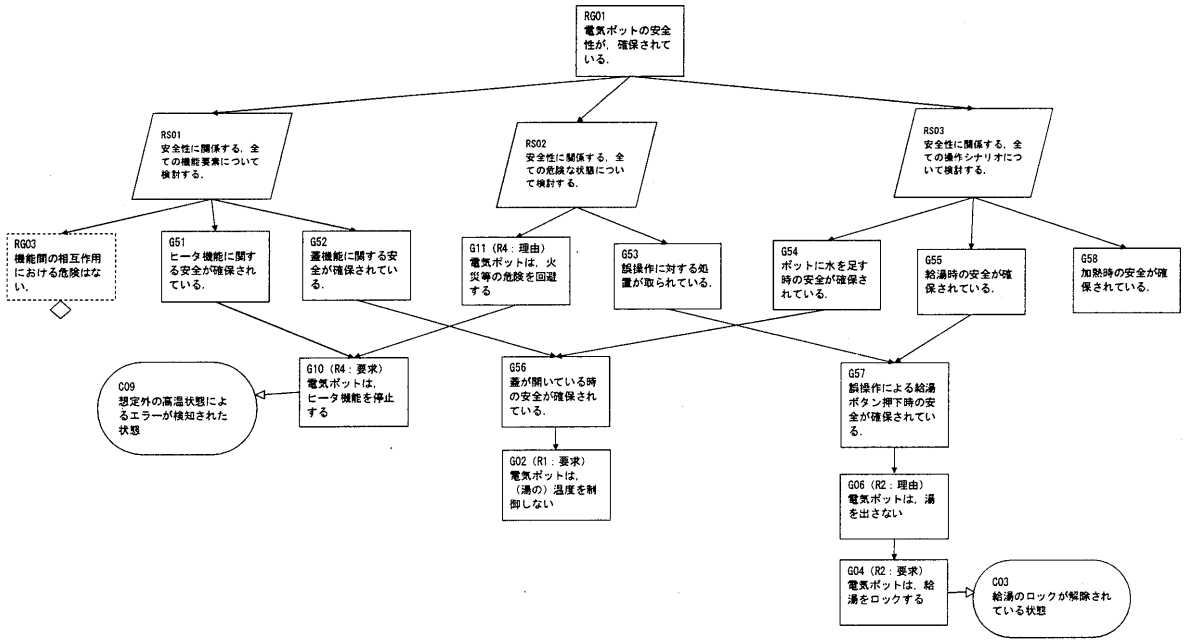

図 6 Assurance Case

手順 2 では，このような Context が付与された Goal が 11 個作成された．

3.2.3. 手順 3

手順 2 で作成した Context が付与された Goal とリファレンスモデル（図 2）を使って構築した Assurance Case を図 6 に示す．ここでは，要求表から抽出された 11 個の Goal のうち，電気ポットの安全性に関する 5 個の Goal を使用している．また，Assurance Case 構築の過程で，8 個の Goal を新規に追加した．Goal に付与されていた Context の内容が上位ゴールで表現されていた場合，冗長となるので Assurance Case のグラフ表記から外した．

作成された Assurance Case は，要求表にある情報のみを使って構築している．また，要求表に含まれる情報のみでは Assurance Case を構築するのに十分であるとは言えない．従って，現実の手法適用場面では，この後の取り組みで作成した Assurance Case の完成度を増していく必要がある．

3.2.4. 対象外となった Goal

手順 3 において，電気ポットの安全性に関する Goal 要素ではないと判断した 6 個の Goal を Assurance Case の対象から外した（表 4）．これら Goal のうち G01，G05，G07，G08 は，安全性以外の機能要求について書かれたものである．G03，G09 は安全性に関する要求であると考えられるが，電気ポットではなく電気ポットメーカーやユーザーなど，他のものが主体となっている安全性要求である．ここでは，電気ポット以外が主体となる安全性に関する要求について区別し，Assurance Case からはずした．

3.3. 適用結果

本稿で提案した手法を，要求表に対して適用することにより，要求表から Dependability に関する情報を抽出し Assurance Case を構築できることが確認された．

表 4 対象外となった Goal 一覧

ID	Goal
G01	電気ポットは，ロックを解除する
G03	電気ポットメーカーは，電気ポットの安全を確保する
G05	電気ポットは，給湯のロックを解除する
G07	電気ポットは，湯を出す
G08	電気ポットは，湯を出す
G09	ユーザーは，やけどをしない

4. 関連研究

近年，Assurance Case に対する研究が，数多く実施されている[1][2][3][4][5]．Assurance Case の構築プロセスに関する研究[2]では，本稿でも使用した，GSN を構築する際 Context を記述ための記法や，GSN のパターンを記述するための記法を導入している．また，Assurance Case 構築の事例研究も実施されている．[1]は，医療機器分野における Assurance Case 構築の事例研究である．これらの研究は，基本的に Assurance Case 構築の手法としての GSN に関する研究である．これに対して，本稿で提案した手法は，情報システム開発で作成される要求表に基づき，GSN を用いて Assurance Case を構築するための手法である．

5. 考察

5.1. 要求分析シートによる要求文の分析

対象を分解して理解する方法に，問題理解のための Problem Flame や，課題分析のための CATWOE などがある．本稿で使用している要求分析シートは，Parnas の 4 変数モデル[8][9]を参考にして考案したものである．4 変数モデルでは，情報システムに対する要求を，利用環境に対する“観測変数”と“制御変数”にわけて整理する．要求分析シートでは，Assurance Case に対する要求を“主体”，“環境”，“操作”，“対象”，“結果”に分解して整理する．ここで“環境”は“観測変数”に，“操作”は“制御変数”に相当すると考えられる．また，GSN における Goal では主体と対象が明確になっていることが重要であることを考慮し，“操作”の“主体”と“対象”についても分割して整理することにした．

5.2. 対象以外の安全性要求

要求表に含まれる安全性に関する要求には，Assurance Case の直接の対象以外に関する安全性の要求が，含まれている場合がある．本稿で示した手法の適用では，表 3 の“G03 電気ポットメーカーは，電気ポットの安全を確保する”や“G09 ユーザーは，やけどをしない”が，このケースに該当すると考えられる．本稿で示した手法の適用では，電気ポットを対象にした Assurance Case を構築している．つまり Assurance Case が直接対象としているのは電気ポットの振る舞いであると考えた．しかし，例えば G09 はユーザーの安全性に関する要求であり，ユーザーが主語となる要求である．従って，G09 は電気ポットの安全性と関係しており，電気ポットの Assurance Case に，その情報を含める選択肢も考えられる．しかし，今回は対象から外した．これらの要求を混在させたままにするより，別途整理した方が良いと判断したためである．このように，異なる Assurance Case の対象を明確に区別して検討できる環境を整えることは，今後の課題である．

6. まとめと今後の課題

本稿では，要求表から要求分析シートにより Dependability に関する情報を抽出し，リファレンスモデルを利用して Assurance Case を構築する手法を提案した．Assurance Case の構築には GSN を利用している．要求表には Dependability に関する情報が含まれている．しかし，その情報は他の要求とともに要求表全体に渡っており，全体像を把握することが難しい．本稿で提案した手法を使用して Assurance Case を構築することで，Dependability に関する情報の全体像を構造的に把握できる．

今後は Assurance Case とアーキテクチャ記述の関係を整理する必要がある．本稿で提案した手法は，システム構築の上流工程で利用できるが，アーキテクチャ記述との関係を整理により，システム設計工程以降でも Assurance Case が意識されるようになり，Assurance Case の形骸化の防止に期待がもてる．また，考察で述べたような，Assurance Case の対象を Assurance Case と統合的に整理する環境の開発も今後の課題の一つとなる．

文　献

[1] Mark-Alexander Sujan, Floor Koornneef, and Udo Voges, Goal-Based Safety Cases for Medical Devices: Opportunities and Challenges, F. Saglietti and N.Oster (Eds.): SAFECOMP 2007, LNCS 4680, pp. 14-27, 2007.

[2] Kelly, Tim P. “Arguing Safety - A Systematic Approach to Safety Case Management,” DPhil Thesis, York University, Department of Computer Science Report YCST, May 1999.

[3] Ankrum, T. Scott and Alfred H. Krombolz. “Structured Assurance Cases:Three Common Standards, “Slides presentation at the Association for Software Quality (ASQ) Section 509 meeting, the MITRE Corporation, 25, January 2006

[4] Bishop, P., Bloomfield, R., Guerra, S.: The Future of Goal-Based Assurance Cases. In:Proc. Workshop on Assurance Cases, pp. 390-395 (2004)

[5] Thomas Rhodes, Frederick Boland, Elizabeth Fong, Michael Kass , Software Assurance Using Structured Assurance Case Models, NIST Interagency Report 7608,

[6] 清水吉男，テストの質を上げるための要求仕様書，JaSST2007 講演資料

[7] 組込みシステム教育教材 話題沸騰ポット GOMA-1015 型 要求仕様書，http://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm

[8] Parnas, D.L. and Madey, J. 1995.Functional documentation for computer systems. Science of Computer Programming, 25(1):41-61.

[9] 山本修一郎，連載要求工学第 4 回要求工学プロセス，2004BUSINESS COMMUNICATION，http://www.bcm.co.jp/site/2005/2005-02/05-youkyuu-kougaku-02/05-youkyuu-kougaku-2.htm