一般
投稿論文

ITシステムを利用するサービスのアシュアランスケース作成

猿渡 卓也[†1]　丹羽　隆[†2]　山本 修一郎[†3]

[†1]名古屋大学／(株) NTTデータ　[†2](株) NTTデータ　[†3]名古屋大学

近年，ITシステムを利用するサービスの障害が，社会的な問題になってきている．このような状況の下で，サービスを保証する手段として，アシュアランスケースが注目されている．筆者らは，実際に企業で使用されているサービスを対象として，これまで適用報告がほとんどなかったエンタープライズ系サービスに対するアシュアランスケースの作成と確認を実施した．その結果，従来の取り組みでは議論・分析が不足していた事項を45個（全体に対する比率で34%）発見・指摘することができた．また，有効性に関するさまざまな知見とともに，アシュアランスケースの作成や評価の手順等に関する知見も得られた．

1. はじめに

ITシステムを利用するサービスの障害が，社会的な問題になってきている．社会的に重要なサービスの障害は，大きな損失をもたらす．複数のITシステムが複雑に相互連携する状況が，この問題への対応をさらに難しくしている．このような状況の下で，システムのディペンダビリティを保証する手段として，アシュアランスケースが注目されている．アシュアランスケースとは，システムのディペンダビリティに関する議論を構造的に記述した文書である．アシュアランスケースは，要件定義から運用に至るシステム開発全般で使用される．アシュアランスケースを使用することにより，システムのディペンダビリティに関する議論を整理し，ステークホルダ間で共有することができる．

従来，組込み系システムに対しては，このようなアシュアランスケースが使用されてきた．この理由として，自動車に搭載されるシステムのように，組込み系システムでは，システムの不具合が重大な損害に直結しやすいことに加え，不具合が発覚してからの修正が困難であることなどが考えられる．しかしながら，エンタープライズ系サービスに対するアシュアランスケースの適用事例はほとんど存在しなかった．エンタープライズ系のサービスやシステムにも社会的に重要なインフラは存在し，その障害が重大な損害を引き起こす可能性がある．そのため，エンタープライズ系サービスにおいても，システムの保証は重要な課題となる．組込み系システムとエンタープライズ系システムにおけるアシュアランスケースの適用に，本質的な違いはないと考えられる．

本稿では，エンタープライズ系サービスを対象にして，アシュアランスケースを作成し確認するプラクティスを紹介する．本稿におけるプラクティスでは，対象サービスの直接のステークホルダではない第三者が主導して，アシュアランスケースを作成する．第三者による作成には，実際の現場に対するアシュアランスケース適用の導入障壁を下げる狙いがある．さらに，本稿におけるプラクティスでは，第三者がアシュアランスケースを使用して，サービスのディペンダビリティについて確認する．

本稿の構成は次の通りである．第2章では，関連研究について述べる．第3章では，d* frameworkについて述べる．d* frameworkとは，アクターを導入したアシュアランスケースの記法であり，本稿で使用されている．第4章と第5章では，本稿におけるプラクティスを，アシュアランスケースの作成とアシュアランスケースの確認に分けて説明する．第6章で考察を述べ，第7章で本稿をまとめる．

2. 関連研究

近年，アシュアランスケースに関する研究が数多く実施されている．アシュアランスケースとは，システムの安全性やディペンダビリティの保証に関する議論を記述した文書である．一般的に，アシュアランスケースは，次のように定義されている[1].

“A documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment.”

アシュアランスケースは，保証対象ごとに異なる名称で呼ばれる場合がある．安全性を対象にしたセーフティケース[2]，ディペンダビリティを対象にしたディペンダビリティケース[3]等の名称がある．ディペンダビリティとは，サービスやシステムの品質に関する属性であり，可用性，信頼性，安全性，統合性，保守性の統合概念として定義されている[4]．本稿では，セーフティケース，ディペンダビリティケース等をまとめてアシュアランスケースと呼ぶ[5]．

一般的にアシュアランスケースには，サービスやシステムの保障に関する議論が構造的に記述される．代表的なアシュアランスケースの記法にGSN（Goal Structuring Notation）[2],[6],[7],[8]，CAE（Claim, Argument, Evidence）[9]がある．GSNでは，4つの要素（ゴール，戦略，証拠，コンテキスト）と2つの関係（“supported by”，“in context of”）を使ってアシュアランスケースが記述される．本稿で使用するd* framework[10],[11]も，アシュアランスケースの記法の1つである．

アシュアランスケースに関する研究に，次のようなものがある．[12]では，アシュアランスケースのパターンに関する研究が実施されている．いくつかのパターンの例が[13],[14]に記載されている．特に，[15]では議論分解のパターンに関する研究が実施されている．また，[16]では議論分解のパターンの効果が評価されている．アシュアランスケースのモジュール化に関する研究も実施されている[17],[18],[19],[20]．アシュアランスケースの作成プロセスについての研究も実施されている．[2],[6]では，6つの手順からなる作成プロセスが提案されている．また，偏差分析を使った方法[21]，シナリオをベースとした方法[18]も提案されている．

従来のアシュアランスケースの研究においても，実際のアシュアランスケースの作成報告は存在する[22]．しかし，エンタープライズ系のサービスを対象としたものは存在しない．また，アクターの概念が導入されているd* frameworkを使ったアシュアランスケースの作成報告も存在しない．本稿では，d* frameworkを使ったエンタープライズ系のサービスにおけるアシュアランスケース作成のプラクティスについて報告する．また，対象サービスの直接のステークホルダではない第三者が主導してアシュアランスケースを作成する際の手順を示し実践している点も，本稿で実施するプラクティスの特徴である．

3. d* framework

d* frameworkとは，筆者らが提案したアシュアランスケースの記法である．この記法は，GSNの拡張として定義されている．d* frameworkにより記述されるアシュアランスケースには，GSNで定義されている要素に加え，アクターの要素が使用される．アクターとはアシュアランスケースが対象としているサービスを構成する要素である．システム，サブシステム，人，組織等がアクターとして定義される．アクターの導入によりd* frameworkでは，アクター間のディペンダビリティとアクター内のディペンダビリティを分けて記述することが可能となる．d* frameworkで記述されるアシュアランスケースには，下記の2種類が存在する．

1. アクターが他のアクターに対して責任を遂行することを示すアシュアランスケース
2. アクター自体がディペンダブルであることを示すアシュアランスケース

アクターが他のアクターに対して責任を遂行することを示すアシュアランスケースの例を図1に示す．また，アクター自体がディペンダブルであることを示すアシュアランスケースの例を図2に示す．アクターが他のアクターに対して責任を遂行することを示すアシュアランスケースには，複数のアクターが定義される．アクター自体がディペンダブルであることを示すアシュアランスケースは，それら複数のアクターに対してそれぞれ個別に作成される．図1では，“ユーザ”と“システム”の2つ

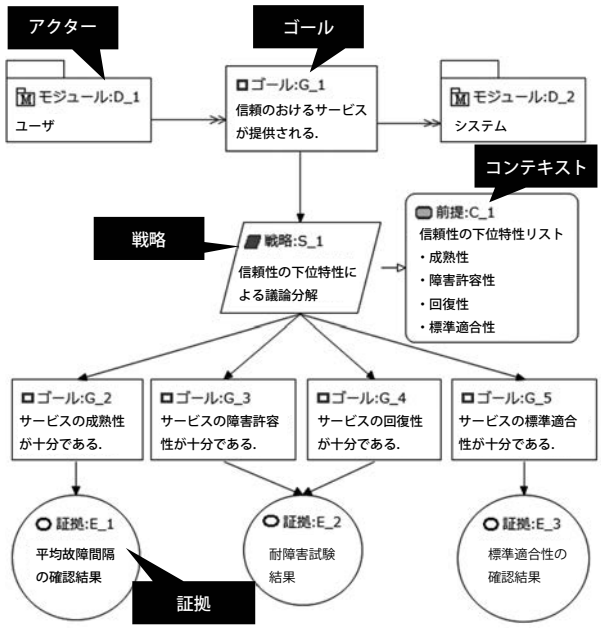

図1　d* framework によるアシュアランスケースの例．（1. アクターが他のアクターに対して責任を遂行することを示すアシュアランスケース）

のアクターが定義されている．図2は，図1で定義されている2つのアクターのうち“システム”について，“システム”自体がディペンダブルであることを示すアシュアランスケースの例である．

4. アシュアランスケースの作成

本稿のプラクティスでは，定義した作成手順を使用して，アシュアランスケースを作成する．また，サービスに直接関係しない第三者が主導して，アシュアランスケースを作成する．本稿で示す作成手順を使用するには，“作成を主導する第三者がアシュアランスケースの作成に精通している”，“ディペンダビリティについて記載された対象サービスの文書が存在し閲覧できる”，“作成されたアシュアランスケースを修正するためにステークホルダの協力が得られる”といった前提条件が存在する．

アシュアランスケースは，要件定義から運用に至るシステム開発工程の全般で使用することができる．本稿では，運用中のサービスに対してアシュアランスケースの作成を実施する．この章では，実施したアシュアランスケースの作成について説明する．

4.1 対象サービスの概要

本稿におけるアシュアランスケースの作成対象は，ITシステムを使ったSIer（System Integrator）の社内向けサービスである．対象としたSIerでは，ITシステム開発プロジェクトの管理を実施するために，このサービスが利用されている．ユーザは，このサービスを利用して，ITシステム開発プロジェクトの進捗管理，品質管理等を実施できる．対象としたSIerでは，このサービスにより，常時500前後のプロジェクトが管理されている．また，このサービスは24時間365日提供されている．

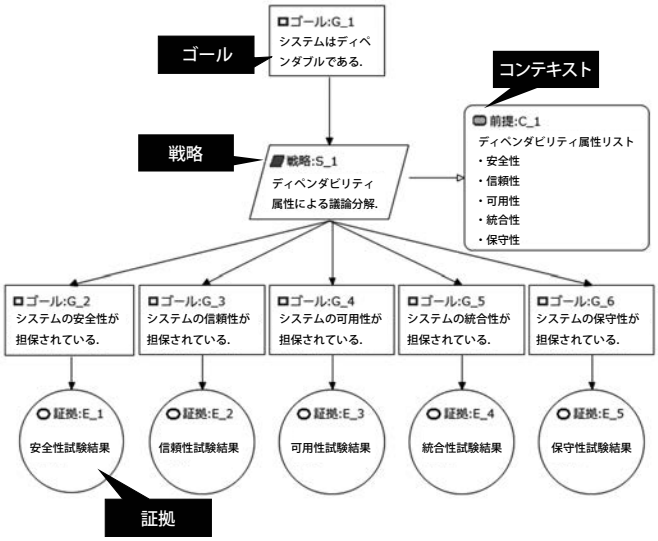

図2　d* framework によるアシュアランスケースの例．（2. アクター自体がディペンダブルであることを示すアシュアランスケース）

4.2 作業者

本稿におけるアシュアランスケースの作成では，サービスに直接かかわっていない第三者が主導するかたちでアシュアランスケースの作成作業を実施する．まず，第三者がアシュアランスケースを作成する．その後，作成されたアシュアランスケースを使用して，サービスにかかわるステークホルダとディスカッションを行い，得られた指摘事項に基づいて第三者がアシュアランスケースを修正する．アシュアランスケースに関する知識が乏しい状態のステークホルダが，アシュアランスケースを作成するのは困難である．本稿では，アシュアランスケースに関する知識を十分に有した第三者が，アシュアランスケースの作成を主導することで，この困難性を克服している．

4.3 作成手順

本稿では，アシュアランスケースを作成するにあたり，複数のステップからなる手順を定義した．以下に各ステップにおける実施内容を示す．

1.　事前準備

1.1　資料確認

本稿におけるアシュアランスケースの作成では，対象となるサービスに関する資料を利用する．このステップでは，それら資料の概要を把握する．

1.2　資料選定

“1.1 資料確認”により概要を把握した資料から，実際にアシュアランスケースの作成に使用する資料を選定する．

1.3　情報記載個所の識別

“1.2 資料選定”により選定された資料から，サービスのディペンダビリティに関係する記述と，資料における記載個所を識別する．さらに，識別された記述を，ゴール，戦略，コンテキスト，証拠の4つのカテゴリに分類する．

2.　アシュアランスケースの記述

2.1　アクターの定義

サービスの全体像が記述されている資料等を利用してアシュアランスケース中のアクターを識別し，定義する．

2.2　アクター間の議論記述

“1.3 情報記載個所の識別”により識別されたアシュアランスケースに関係する記述を利用して，アクター間で

必要となるディペンダビリティに関する議論を検討し，アシュアランスケースに記述する．

2.3　アクター内の議論記述

“1.3 情報記載個所の識別”により識別されたアシュアランスケースに関係する記述を利用して，アクター内で必要となるディペンダビリティに関する議論を検討し，アシュアランスケースに記述する．

3.　アシュアランスケースの修正

3.1　ディスカッション

“2. アシュアランスケースの記述”により作成されたアシュアランスケースを使用して，サービスに直接かかわっているステークホルダとディスカッションを実施し，記述の誤り，記述の漏れ等に関して確認する．

3.2　記述修正

“3.1 ディスカッション”の結果に基づいて，アシュアランスケースを修正する．

4.4　作成に使用した資料

本稿におけるプラクティスでは，対象となるサービスに関する資料を使用してアシュアランスケースを作成する．上記の作成手順“1.1 資料確認”，“1.2 資料選定”を経て，対象サービスに関する 172 個の資料から 11 個の資料が，アシュアランスケースの作成に使用する資料として選定された．選定された資料の一覧を**表 1** に示す．

4.5　作成結果

4.3 節の作成手順に従い，対象となるサービスに対して，アクターが他のアクターに対して責任を遂行することを示すアシュアランスケースと，アクター自体がディペンダブルであることを示すアシュアランスケースを作成した．ここでは，作成した各アシュアランスケースに対して“サービス”，“IT システム”という名称を使用する．

表 1　作成に使用した資料一覧

項番	資料名	ページ数
1	バックアップ管理対象一覧	3
2	バックアップ・リストア設計 _ 詳細設計書	59
3	性能要件	12
4	信頼性要件	4
5	システム運用管理要件	11
6	運用・保守性検討書	3
7	可用性検討書	6
8	性能・拡張性検討書	3
9	運用・保守性要件一覧	2
10	可用性要件一覧	2
11	性能・拡張性要件一覧	2

4.5.1　アシュアランスケースのノードの個数

作成されたアシュアランスケースのノードの個数を，2 つのアシュアランスケースおよびノードの種類ごとに整理したものを**表 2** に示す．表 2 では上記作成手順における“2. アシュアランスケースの記述”の結果と“3. アシュアランスケースの修正”の結果を，それぞれ作成後欄と修正後欄に示している．表から，本稿におけるプラクティスでは，第三者のみによるアシュアランスケースの作成において，ノード数 42（サービス）とノード数 54（IT システム）の 2 つのアシュアランスケースが作成されたことが分かる．また，ステークホルダとディスカッションを実施しアシュアランスケースの記述を修正した結果，ノード数が 1.375 倍に増加し，最終的にノード数 60（サービス）と，ノード数 72（IT システム）の 2 つのアシュアランスケースが作成されたことが分かる．

4.5.2　アクターが他のアクターに対して責任を遂行することを示すアシュアランスケース（サービス）

この節では，本プラクティスにおいて作成した，アクターが他のアクターに対して責任を遂行することを示すアシュアランスケースについて説明する．このアシュアランスケースには，利用者，IT システム，システム開発者，システム運用者の 4 つのアクターと，アクター間の責任関係に関する議論が定義されている．アクター間の責任関係として，利用者から IT システムに対するサービス信頼性責任に関する責任関係，IT システムからシステム開発者に対する開発責任に関する責任関係等が定義されている．作成したアシュアランスケースの一部を**図 3** に示す．ここでは，利用者から IT システムに対するサービス信頼性責任に関する議論が定義されている．利用者から IT システムに依存する関係として“信頼のおけるサービスが提供されている”というゴールが定義され，信頼性の下位特性によって議論が分解されている．このように，アクターが他のアクターに対して責任を遂行す

表 2　作成されたアシュアランスケースのノード個数

アシュアランスケース	ノード	個数	
		作成後	修正後
サービス	アクター	4	4
	ゴール	29	37
	戦略	3	6
	証拠	6	13
	合計	42	60
IT システム	ゴール	44	56
	戦略	7	10
	コンテキスト	3	3
	証拠	0	3
	合計	54	72

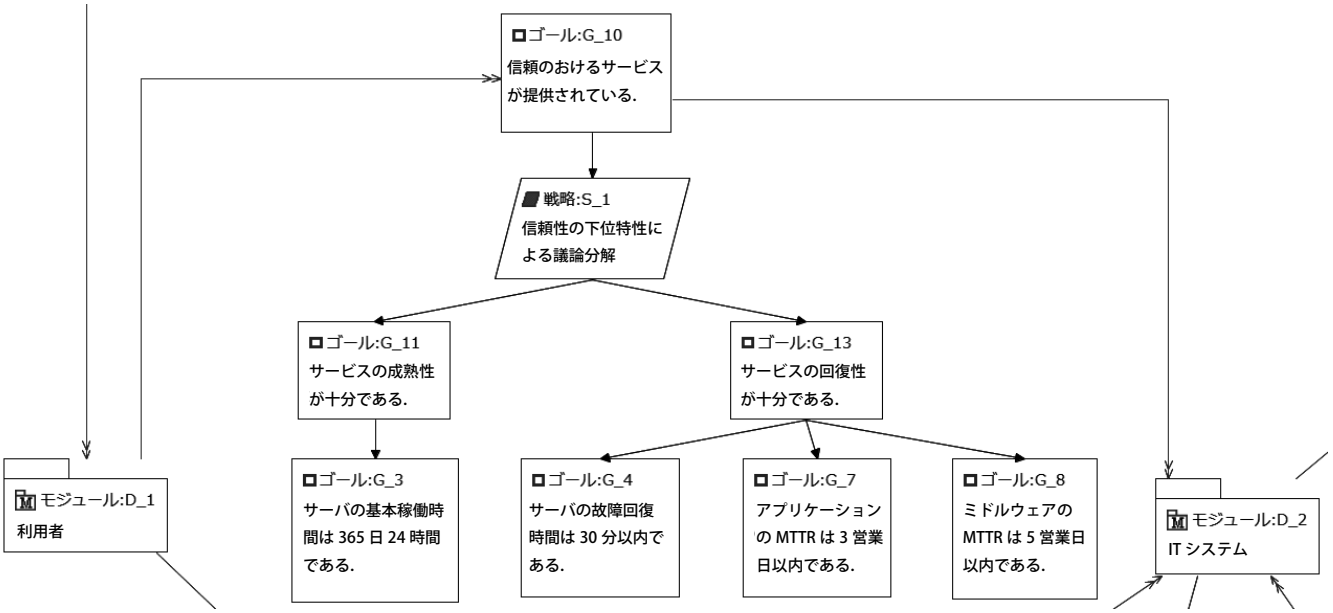

図 3　アシュアランスケースからの抜粋　利用者と IT システム間のサービス信頼性責任に関する責任関係の議論

ることを示すアシュアランスケースには，アクター間の責任関係に関する議論が構造的に定義される．

4.5.3　アクターがディペンダブルであることを示すアシュアランスケース（IT システム）

この節では，本稿で作成した，アクターがディペンダブルであることを示すアシュアランスケースについて説明する．このアシュアランスケースの対象は，アクターが他のアクターに対して責任を遂行することを示すアシュアランスケース（サービス）においてアクターとして定義されている IT システムである．IT システムは，アクターが他のアクターに対して責任を遂行することを示すアシュアランスケース（サービス）内で定義されている 4 つのアクターのうちの 1 つである．他のアクターについては，アシュアランスケースを作成するための入力情報となる資料が存在しなかったため，今回は作成していない．作成したアシュアランスケースでは，可用性，信頼性, 性能に関する議論が実施されている．すなわち，このアシュアランスケースでは，“システムの可用性が担保されている”，“システムの信頼性が担保されている”，“システムの性能が担保されている”の 3 つのゴールを分解することで議論がすすめられている．図 4 に IT システムの信頼性に関して議論分解を行ったアシュアランスケースの一部を示す．ここでは，信頼性に関する議論として，“システムの信頼性が担保されている”というゴールが定義されている．さらに，ハードウェアとソフトウェアに分けて議論する戦略に沿って，2 つのゴールが定義されている．

図 5 に，バックアップの取得に関する議論を示すアシュアランスケースの一部を示す．これは，図 4 で示した信頼性の担保に関する議論の下位で実施されている議論である．“バックアップを取得する”というゴールが定義され，対象機器ごとに分解する戦略に沿って議論が進められている．また，議論を分解する戦略には対象機器のリストがコンテキストとして付与されている．

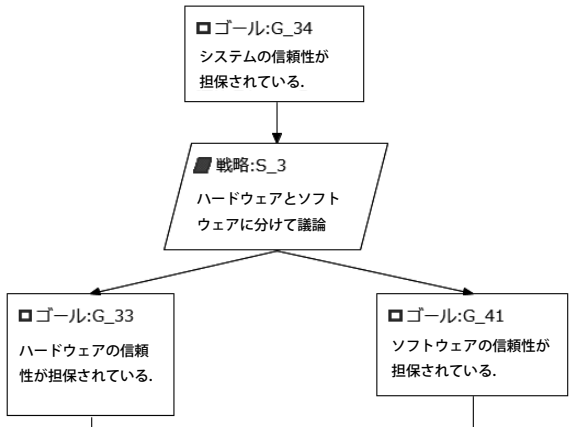

図 4　アシュアランスケースからの抜粋 信頼性の担保に関する議論

4.6　作業時間

アシュアランスケースの作成手順ごとに，作業時間を計測した結果を表 3 に示す．本稿で実施したプラクティスに費やした作業時間は全体で 14 時間であった．“3.1 ディスカッション”の 1 時間以外は，ステークホルダ以外の第三者 1 人による作業時間である．

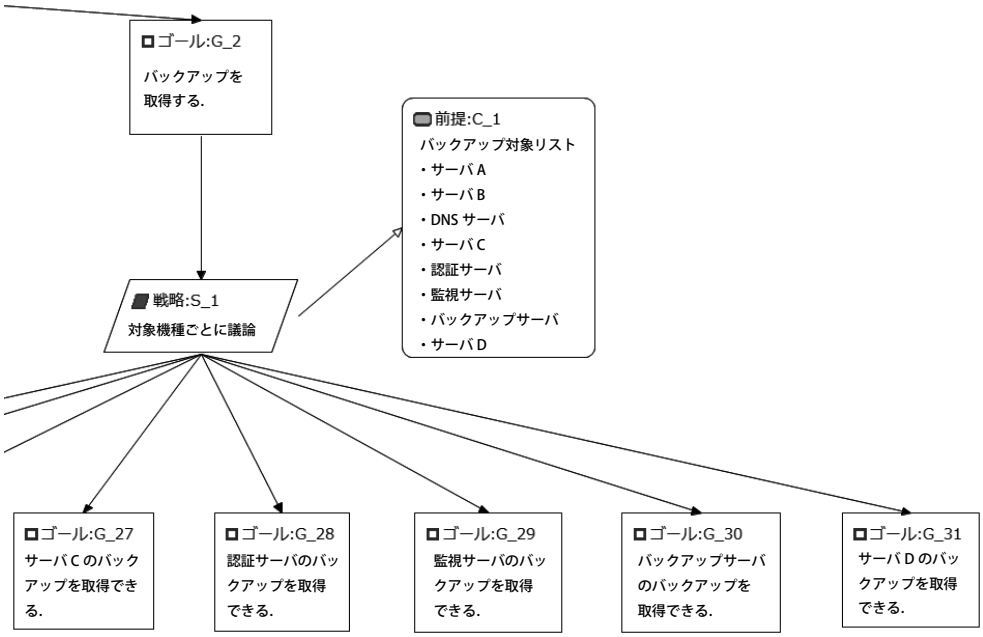

図 5　アシュアランスケースからの抜粋バックアップの取得に関する議論

表 3　アシュアランスケース作成に要した作業時間

作業手順		作業時間
1 事前準備	1.1 資料確認	2 時間
	1.2 資料選定	10 分
	1.3 情報記載個所の識別	1 時間 50 分
2 アシュアランスケース記述	2.1 アクターの定義	20 分
	2.2 アクター間の議論記述	2 時間
	2.3 アクター内の議論記述	3 時間 40 分
3 アシュアランスケース修正	3.1 ディスカッション	1 時間
	3.2 記述修正	3 時間

5. アシュアランスケースの確認

この章では，本稿で実施したアシュアランスケースの確認について説明する．本稿のプラクティスにおいて作成したアシュアランスケースには，作成に使用した資料およびステークホルダとのディスカッションで明らかにできなかった議論の不足個所が存在することが考えられる．本稿におけるプラクティスでは，アシュアランスケースの構造に着目した次の3つの観点を利用することにより，第三者によるアシュアランスケースの議論の不足個所を指摘する確認を実施した．

1.「証拠の不足個所」の確認

アシュアランスケースにおいて，議論を保証する証拠が不足している個所がある．そのような個所を「証拠の不足個所」として指摘する．**図6**に「証拠の不足個所」の例を示す．この例では，最下層のゴールに対して，そのゴールを保証する証拠が不足している．

2.「議論の不足個所」の確認

アシュアランスケースにおいて，上位のゴールが下位のゴールに十分に分解されていない個所がある．そのような個所を「議論の不足個所」として指摘する．**図7**に「議論の不足個所」の例を示す．この例におけるゴールG_39は，議論の分解が不十分である．

3.「議論分解妥当性の不足個所」の確認

アシュアランスケースにおいて，議論分解に対する戦略に，適切なコンテキストが付与されていない個所がある．そのような場合，議論分解の妥当性が不足していると判断できる．ここでは，“対象機器ごとに議論”など，アシュアランスケースの対象に固有な議論分解個所について，コンテキストが不十分である個所を「議論分解妥当性の不足個所」として指摘する．**図8**に「議論分解妥当性の不足個所」の例を示す．この例の戦略は，対象に固有な議論分解の戦略であるにもかかわらず，適切なコンテキストが付与されていない．

作成したアシュアランスケースを用いて実施した，第三者によるサービスのディペンダビリティに関する議論の不足個所の指摘結果を**表4**に示す．表4では，アクター間の責任関係を示すアシュアランスケース（サービス）と，アクターがディペンダブルであることを示すアシュアランスケース（ITシステム）に分けて不足個所の個数を示した．また，アシュアランスケースに含まれる要素の個数に対する不足個所の個数の割合も示している．表より，アクター間の責任関係を示すアシュアランスケースに13個（22%），アクターがディペンダブルであることを示すアシュアランスケースに32個（44%）の合計45個（34%）の議論の不足個所を指摘できたことが分かる．

今回のプラクティスにおいて指摘された議論の不足個所は，比較的単純なものである．しかし，アシュアランスケースの作成に使用した資料からは漏れていた議論であり，今回のプラクティスのような，サービスの保証に関する議論の体系的な整理がなければ，見落とされていたものである．アシュアランスケースを作成し，体系的に議論を整理することにより，比較的短い時間でこれら

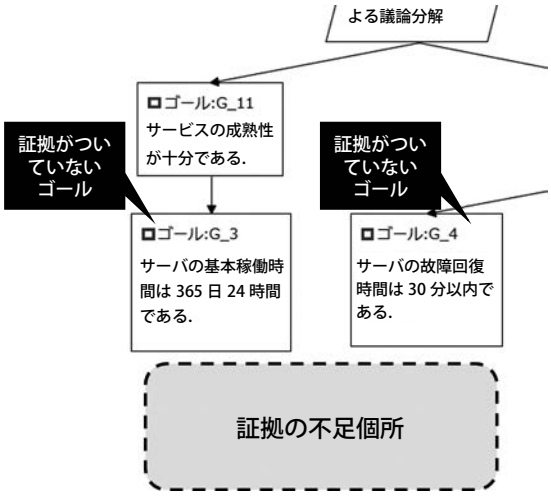

図 6　証拠の不足個所の例

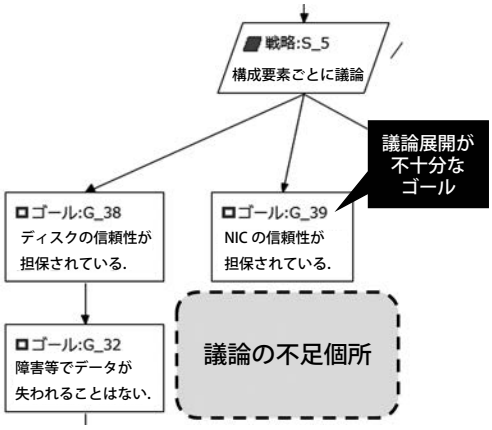

図 7　議論の不足個所の例

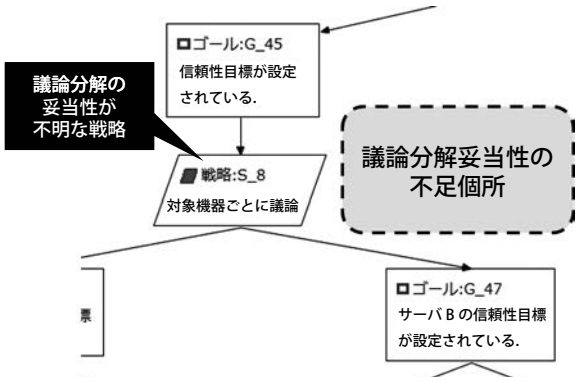

図 8　議論分解妥当性の不足個所の例

表 4　アシュアランスケースの確認結果

確認の観点	サービス		IT システム		合計	
	個数	割合	個数	割合	個数	割合
1 証拠の不足個所	8	13%	25	35%	33	25%
2 議論の不足個所	4	7%	4	6%	8	6%
3 議論分解妥当性の不足	1	2%	3	4%	4	3%
合計	13	22%	32	44%	45	34%

の不備が発見できたことから，今回のアシュアランスケースの作成が有益であったと考えることができる．

6. 考察

6.1　ステークホルダによる評価

本稿で実施したプラクティスでは，アシュアランスケースの確認後，実際にサービスにかかわっているステークホルダからコメントを収集した．得られたコメントを表 5 に示す．これらのコメントから，以下の知見が得られた．アシュアランスケースに記述されている内容は容易に理解することができる．また，十分な知識があればステークホルダ自身でアシュアランスケースを作成することもできる（C01，C02，C03）．社会インフラ等のミッション・クリティカルなシステムが関係するサービスを対象とした方が，そうではないサービスを対象とするよりも，アシュアランスケースを有効に活用できると考えられる．また，そのようなサービスであれば，アシュアランスケースの作成コストも許容できると考えられる．ただし，監査等の明確な目的があれば，一般的なサービスにおいてもアシュアランスケースは有効であると考えられる（C04，C05，C08）．サービス開発の上流工

表 5　プラクティスおよびアシュアランスケースに対するステークホルダのコメント

ID	コメント
C01	サービスのディペンダビリティに関する情報を，このように整理したことはなかった．
C02	作成されたアシュアランスケースについては，構造化されていたので理解できた．また，アクター同士の関係についても理解できた．
C03	整理学等の作成のための知識があれば，担当内（ステークホルダ自身）でもアシュアランスケースの作成は可能である．
C04	今回作成したアシュアランスケースは，手段指向で作成しているので，直接役に立っているとはいえない．しかし，監査等の明確な目的があれば役に立つ可能性はある．
C05	銀行のシステム，防衛分野，航空管制，社会インフラ等のクリティカルなシステムの方が，アシュアランスケースを役立てることができると考えられる．
C06	企画，要件定義工程における活用の方が，アシュアランスケースを役立てることができると考えられる．
C07	システム開発者だけでアシュアランスケースを作成すると，その枠内のみの議論になってしまうという問題がある．
C08	アシュアランスケースを作るための工数が導入障壁になると考えられる．品質レビュー等に多くの時間を割いているシステムでは，導入が可能かもしれない．
C09	マネージャー等の上位層に対する価値の説明が難しいという問題がある．
C10	関係者が多くなると，作成が困難になる可能性があると考えられる．
C11	アシュアランスケースが大きくなり過ぎると，作成が困難になる可能性があると考えられる．

程の方が，アシュアランスケースの有効性を活かすことができる（C06）．アシュアランスケースの導入障壁として「作成コストがかかる」,「関係者への説明が難しい」という問題がある（C08，C09）．しかし，作成コストについては，導入サービスを適切に選択すれば問題にならない可能性がある（C05）．

また，アシュアランスケースの作成に関する課題として，「関係者の増加による作成の困難さの増大の克服」,「アシュアランスケースの肥大化に伴う作成の困難さの増大の克服」が挙げられている（C10，C11）．これらのうち，アシュアランスケースの肥大化については，アシュアランスケースをモジュールに分割して記述する方法が提案されている[17],[18],[19],[20]．しかし，アシュアランスケースをモジュールに分割するだけでは，アシュアランスケースが意味のあるまとまりとして適切に分割されない可能性がある．本稿で使用したd* frameworkは，アシュアランスケースをアクターに分割して管理する．これは，アシュアランスケースを，まとまった意味を持つアクターという単位に分割して管理する手法である．したがって，d* frameworkにより，肥大化するアシュアランスケースを適切に分割して管理することができると考えられる．

6.2　従来の取り組みとの比較

従来，サービスあるいはシステムの保証に関する議論が明示的に示されているケースは少なかった．アシュアランスケースは，このようなサービスやシステムの保証に関する議論を文書化することで，明示的に示すための技術である．すなわち，従来の取り組みと比較すると，アシュアランスケースを使用することにより，サービスあるいはシステムの保証に関する議論を明示的に示すことができるという点で異なる．議論を明示的に示すことにより，サービスやシステムの保証に関する議論や対策をステークホルダ間で共有でき，議論の漏れを明確にできる．本プラクティスでは表4に示すとおり，アシュアランスケースにおける45個の不足個所を指摘することができた．これらの指摘個所は，サービスのディペンダビリティを確保するために議論が必要な個所であり，従来の取り組みでは見過ごされていたと考えることができる．つまり，アシュアランスケースを使用することにより，従来の取り組みでは見過ごされていた，サービスのディペンダビリティを保障する上で必要な議論の発見につながったと考えることができる．

6.3　他手法との関係

アシュアランスケースは，要求定義手法，設計手法，試験手法のようなシステム開発における他の既存手法に置き換わる技術ではない．アシュアランスケースは，サービスやシステムを保証するための議論を構造的に整理するための技術である．既存手法において作成されるドキュメントは，アシュアランスケースにおける議論を保証するための証拠となり得る．また，既存手法で作成されるドキュメントを，アシュアランスケースを使って保証するという関係もあり得る．今後UML（Unified Modeling Language）のような既存手法におけるドキュメントとアシュアランスケースの関係を，体系的に整理する必要がある．

6.4　エンタープライズ系情報サービスを対象としたアシュアランスケース

これまで，アシュアランスケースの適用対象は，組込み系のシステムが中心であった．この理由として，システムの不具合が直接重大な損害に直結しやすいことや，リリース後の修正が困難であるという組込み系のシステムが持つ特性が考えられる．本稿では，SIerにおけるITシステムを使用した社内向けサービスを対象として，アシュアランスケースを作成した．その結果，エンタープライズ系サービスについても，アシュアランスケースの作成が有効であるというステークホルダの評価が得られた（表5）．

6.5　第三者によるアシュアランスケースの作成

サービスオーナー，顧客，サービス提供者，システム開発者等の実際のサービスにかかわっているステークホルダが，アシュアランスケースに関する知識が乏しい状況でアシュアランスケースを作成するのは困難である．そこで，本稿では，サービスに直接関係していない第三者が主導してアシュアランスケースを作成した．この第三者は，対象サービスに直接関係していないが，アシュアランスケースについて十分な知識を持つ者である．本稿では，直接のステークホルダではない第三者によるアシュアランスケースの作成を可能とするため，アシュアランスケースの作成手順を定義し使用した．この作成手順では，アシュアランスケースを作成するための入力情報として，サービスに関係する資料を利用した．その結果，実際のステークホルダから見ても違和感のないアシュアランスケースを作成することができた．これは，ステークホルダによる評価からも分かる（表5）．すなわち，

本稿で提示した手順によって，直接サービスに関係していない第三者が対象サービスのアシュアランスケースを構築できるという知見が得られた．

表5のコメントから，今回のプラクティスを実施することで，ステークホルダのアシュアランスケースに対する理解が高まったことが分かる．また十分な学習を積めば，ステークホルダもアシュアランスケースを作成でき，対象サービスの高信頼化に役立つと考えていることが分かった．ステークホルダが自らアシュアランスケースを作成する利点は，自分たちの実施するサービスの保証に関する議論を直接アシュアランスケースとして記述できる点である．第三者が主導するアシュアランスケースの作成では，第三者が間に入るというロスが生じる．また，第三者には，アシュアランスケースに対する十分な知識に加え，一般的なシステム開発文書の読解力，ステークホルダとのディスカッションを主導する能力等も必要になる．しかし，第三者が主導することでアシュアランスケース作成の障壁を下げ，中立的な視点でアシュアランスケースを作成できるという利点がある．今後は，これらのトレードオフを考慮した上で，状況に応じたアシュアランスケースの作成が必要になることが考えられる．

6.6 アシュアランスケースの作成手順

サービスに直接関係していない第三者が，サービスに関係する膨大な資料を使って，アシュアランスケースを作成するのは困難である．そのため，本稿では，サービスに関係する文書から第三者がアシュアランスケースを作成する手順を，明確にした．今回この手順を使用することで適切なアシュアランスケースを作成することができた．このことから，他のサービスについても，この作成手順を使用することにより，適切なアシュアランスケースを作成できると考えられる．

6.7 アシュアランスケースの作成時間

今回のプラクティスでは，アシュアランスケースを作成する際の作成時間を測定した．その結果，作成に要した時間は14時間だったことが分かった（表3）．1日の作業時間を5時間程度で見積もると，これは約3営業日に換算でき，比較的短い時間でアシュアランスケースを作成できたことが分かる．ただし，今回のプラクティスにおいて実際作成に使用されたドキュメントは，全体で107ページ（表1）であり大規模なものではなかった．そのため，比較的短い時間でアシュアランスケースを作成することができたと考えられる面もある．より大規模・複雑なサービスやシステムにおいて，アシュアランスケースの作成に要する時間がどのような規模に増大していくのかを，今後，明らかにしていく必要がある．

6.8 第三者によるアシュアランスケースの確認

本稿では，サービスに直接かかわっているステークホルダではなく，第三者によるアシュアランスケースの確認を実施した．アシュアランスケースの持つ構造的な特徴を利用した結果，議論の不足個所が全体で45カ所あることが分かった（表4）．すなわち，アシュアランスケースを利用することで，第三者がサービスのディペンダビリティを確認できるということが分かった．

第三者が指摘した議論の不足個所は，ステークホルダが議論を実施し，補っていく必要がある個所である．このように，アシュアランスケースを使用することによるサービスのディペンダビリティの向上が，第三者においても可能であることが明らかになった．

6.9 限界

- 本稿では，1つのプラクティスしか実施できていない．エンタープライズ系サービスに対するアシュアランスケースの作成事例，および第三者によるアシュアランスケースの作成事例の数としては，少ないという限界がある．
- 本稿で実施したプラクティスは，SIerにおける社内サービスを対象としている．これは，対象の企業にとっては重要なサービスであるが，社会的に重大な影響を持つサービスではない．今回のプラクティスは，社会的に重要なサービスに対しての適用事例ではないという限界がある．

7. おわりに

本稿では，エンタープライズ系サービスに対してアシュアランスケースを作成するプラクティスを実施した．本稿におけるプラクティスでは，サービスに直接関係していない第三者によるアシュアランスケースの作成を試みた．第三者によるアシュアランスケースの作成を可能とするため，事前に作成手順を定義し，その手順を使用してアシュアランスケースを作成した．その結果，サービスに関係するステークホルダからも納得感を得られるアシュアランスケースが，第三者により作成できるという知見が得られた．さらに，アシュアランスケースの構造的な特徴を利用することにより，第三者によるサービ

スのディペンダビリティに関する確認が可能であるという知見も得られた．

今後は，今回実施したようなプラクティスを他の事例でも実施し，アシュアランスケースの適用事例を増やしていく必要がある．それらのプラクティスを重ねることにより，新しい知見が獲得できることが期待できる．また，本稿で示したアシュアランスケースの作成手順は，他の事例にも適用し改善する必要がある．

謝辞

本研究を進めるにあたり，さまざまなご支援をいただいた（株）NTTデータの，木谷強氏，渡辺真太郎氏，堀口智久氏，荻野広樹氏に感謝の意を表します．

参考文献

1) Ankrum, T. S. and Krombolz, A. H.: Structured Assurance Cases: Three Common Standards, Slides Presentation at the Association for Software Quality (ASQ) Section 509 meeting (2006).
2) Kelly, T.: Arguing Safety - A Systematic Approach to Managing Safety Cases, Unpublished Doctoral Dissertation, University of York (1998).
3) Despotou, G. and Kelly, T.: Extending the Safety Case Concept to Address Dependability, in Proceedings of the 22nd International System Safety Conference (2004).
4) Avizienis, A., Laprie, J., Randell, B. and Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing, Dependable and Secure Computing, Vol.1, pp.11-33 (2004).
5) Howell, C. C., Guerra, S., Pfleeger, S. L. and Stavridou-Coleman, V.: Workshop on Assurance Cases: Best Practices, Possible Obstacles and Future Opportunities, in Proc. of the 2004 International Conference on Dependable Systems and Networks (DSN' 04), Florence, Italy (2004).
6) Kelly, T.: A Six-Step Method for Developing Arguments in the Goal Structuring Notation (GSN), Technical Report, York Software Engineering, UK (1999).
7) The GSN Working Group Online: GSN Standard, http://www.goalstructuringnotation.info/
8) Jackson, D., Thomas, M. and Millett, L. I.: Software for Dependable Systems: Sufficient Evidence?, National Research Council (2007).
9) Adelard: ASCE, http://www.adelard.com/web/hnav/ASCE/
10) Yamamoto, S. and Matsuno, Y. : d*framework: Inter Dependency Model for Dependability, DSN 2012 (2012).
11) Saruwatari, T. and Yamamoto, S. : Definition and Application of an Assurance Case Development Method (d*), SpringerPlus 2.1 (2013).
12) Kelly, T. and Weaver, R.: The Goal Structuring Notation - A Safety Argument Notation, Proc. of Dependable Systems and Networks 2004 Workshop on Assurance Cases (2004).
13) Alexander, R., Kelly, T., Kurd, Z. and McDermid, J.: Safety Cases for Advanced Control Software: Safety Case Patterns, Technical Report, Department of Computer Science, University of York (2007).
14) Weaver, R. A.: The Safety of Software? Constructing and Assuring Arguments, Unpublished Doctoral Dissertation, Department of Computer Science, University of York (2003).
15) Bloomfield, R. and Bishop, P.: Safety and Assurance Cases: Past, Present and Possible Future? an Adelard Perspective, in Proceedings of 18th Safety-Critical Systems Symposium (2010).
16) Yamamoto, S. and Matsuno, Y.: An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case, In Proceedings of ASSURE2013, Co-Located ICSE2013, San Francisco, CA, USA (2013).
17) Bate, I. and Kelly, T.: Architectural Considerations in the Certification of Modular Systems, RELIABILITY ENGINEERING & SYSTEM SAFETY, vol.81, pp.303-324 (2003).
18) Kelly, T.: Using Software Architecture Techniques to Support the Modular Certification of Safety-Critical Systems, SCS '06 Proceedings of the Eleventh Australian Workshop on Safety Critical Systems and Software, Australia (2005).
19) Fenn, J., Hawkins, R., Williams, P. and Kelly, T.: Safety Case Composition Using Contracts? Refinements Based on Feedback from an Industrial Case Study, In Proceedings of 15th Safety Critical Systems Symposium (SSS '07), Springer (2007).
20) Kelly, T.: Modular Certification to Support Open Systems Dependability, In the 2nd International Workshop on Open Systems Dependability (WOSD2012) (2012).
21) Despotou, G. and Kelly, T.: EXTENDING SAFETY DEVIATION ANALYSIS TECHNIQUES TO ELICIT FLEXIBLE DEPENDABILITY REQUIREMENTS, System Safety, 2006. The 1st Institution of Engineering and Technology International Conference (2006).
22) Sujan, M. A., Koornneef, F. and Voges, U.: Goal-based Safety Cases for Medical Devices: Opportunities and Challenges, Computer Safety, Reliability, and Security. Springer Berlin Heidelberg (2007).

猿渡 卓也（正会員）saruwatari.takuya@e.mbox.nagoya-u.ac.jp
1996年筑波大学大学院理工学研究科修士課程修了．同年NTTデータ通信（株）入社．2011年名古屋大学大学院情報科学研究科後期博士課程入学．

丹羽　隆（非会員）niwat@nttdata.co.jp
1994年東京工業大学工学部電気電子工学科卒業．同年NTTデータ通信（株）入社．2013年（株）NTTデータ技術開発本部ALMソリューションセンタ部長．

山本 修一郎（正会員）yamamotosui@icts.nagoya-u.ac.jp
1979年名古屋大学大学院工学研究科情報工学専攻修了．同年日本電信電話公社入社．2002年（株）NTTデータ技術開発本部副本部長．2007年同社初代フェロー，システム科学研究所所長．2009年名古屋大学情報連携統括本部情報戦略室教授．AEA JAPAN会長．IPA SEC要求発展型開発WGリーダ．博士（工学）．

投稿受付：2014年4月30日
採録決定：2014年12月18日
編集担当：西　直樹（日本電気（株））