神奈川大学大学院　理学研究科

2017 年度　博士論文

論文題目

システムアシュランス議論のための
オントロジー構築法

2018 年 1 月 15 日 提出

木下 修司

目次

図一覧

表一覧

1. はじめに

本論文は、システムアシュランス議論をより効果的に行うための、システムのオントロジー構築法の研究をまとめたものである。特に、システムライフサイクルプロセスをオントロジーとして記述するための枠組みとして「6W1H モデル」を提案し、その有効性を事例研究によって確かめた。

システムアシュランス議論とは、ある「システム」が望ましい特定の「性質」をもつということを、明確な証拠とともに主張し、ステークホルダ間でアシュランスを得る議論（2.1.2 節）である。より深い確信を得るためには、システムそのものだけでなく、システムライフサイクル（システムの企画・開発・運用等における人間の作業全体）を議論の対象とすることが必要である。

システムアシュランス議論は「アシュランスケース」という文書一式として記録されることが広く行われている。アシュランスケースにおける議論の構造を表現するための様々な図式法が提案されている。また、アシュランスケースを形式理論とその証明として捉える形式アシュランスケースと、そのプログラミング言語 Agda による実装は、アシュランスケースの整合性を自動検査可能にした。

システムアシュランス議論を行い、アシュランスケースとして記録するにあたって、システムライフサイクルにおける個々の活動（システムライフサイクルプロセス）を、議論におけるオントロジー（語彙とその基本的性質）として明らかにすることが重要である。しかし、個々の具体的なシステムライフサイクルにおけるシステムライフサイクルプロセスのオントロジーを記述する方法は確立されておらず、自明ではない。国際標準 ISO/IEC/IEEE 15288 はシステムライフサイクルプロセスの一般的枠組を与えるもので、広く受け入れられているが、具体的なシステムライフサイクルプロセスの記述法を与えるものではない。

そこで本論文では、システムライフサイクルプロセス記述の枠組みとして「6W1H モデル」を提案する。6W1H モデルとは、「6 つの W（Who、What、Whom、Where、When、Why）で表現される人間の作業」をノードとする木である。1 つの作業を記述したノードは、「How」（どのようにその作業を実施するか？）を検討することで、より詳細なレベルの複数の作業に分割される。これにより、システムに関する既存の記述から、システムライフサイクルプロセスを構造的に抽出できる。

また、本論文では、自治体防災業務のオープンシステム・ディペンダビリティに対するアシュランス議論を対象として、6W1H モデルの事例を提供する。地域防災計画と呼ばれる自治体防災業務が定めた文書から、6W1H モデルを用いてプロセス記述を作成し、このプロセス記述に関するアシュランスケースを例示した。

以降の本論文の構成を記す。まず第 2 章では、研究の背景となるシステムアシュランス議論、およびその記録方式アシュランスケースを説明する。第 3 章では、アシュランスケースにおける、システムライフサイクルプロセスのオントロジー構築という課題を説明する。

第 4 章では、本研究の中心であるシステムライフサイクルプロセスのオントロジー構築法を、新たに考案した 6W1H モデルを中心に述べる。第 5 章では事例研究として、考案した 6W1H モデルを自治体の防災業務に適用し、システムアシュランス議論のためのオントロジー構築を試みる。第 6 章で総括し、今後の展望を述べる。

2. 背景：アシュランスケースを用いたシステムアシュランス議論

本章では、研究の背景として、アシュランスケースを用いたシステムアシュランス議論を説明する。システムアシュランス議論は、あるシステムが、望ましい特定の性質（例えば、安全性、セキュア性、信頼性）を確かにもつことを、明確な証拠とともに主張する議論である。ここで重要なのは、「システム」と「システムの性質」という２つの概念があり、それらを区別することである。システムのステークホルダ（利害関係者）によるシステムアシュランス議論の結果は、アシュランスケースと呼ばれる文書一式として記録されるのが一般である。

まず、システムアシュランス議論に関する用語定義を吟味する。次に、アシュランスケースとその発展を概観する。

2.1. システムアシュランス議論

2.1.1. システムとは何か

「システムアシュランス議論」を説明する前に、まず「システム」の定義をする。「システム」という用語は文脈によって様々な意味で用いられるためである。ここでは、システムエンジニアリング分野におけるシステムの定義を中心に概観する。

本論文においては、システムエンジニアリングにおける「システムライフサイクルプロセス」を定める国際標準 ISO/IEC/IEEE 15288 [1]における「システム」の定義を用いる。システムライフサイクルの詳細は後述する。「システム」という用語は、この標準では以下のように定義されている（以下、引用箇所の日本語訳はすべて著者による）。

> system -- combination of interacting elements organized to achieve one or more stated purposes（システム -- 明示された１つ以上の目的を達成するために構成された、相互に作用する要素の組み合わせ）(4.1.46)

また、システム要素（system elements）は、以下のように定義されている。

> system element – member of a set of elements that constitutes a system
> EXAMPLE Hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities or any combination.
> （システム要素 -- システムを構成する要素の集まりの１つ。例：ハードウェア、ソフトウェア、データ、人間、プロセス群（ユーザにサービスを提供する

プロセスなど)、手続き（オペレータの操作など)、機材、物資、天然資源や、それらの組み合わせ）(4.1.47)

まず、システムとは、何かしらの目的を達成されるために構成されるものとしている。明記されていないが、ここでいうシステムは、自然界の生物がもつシステム等ではなく、人間が作るものを想定している。本論文における「システム」も、人間が作るシステムのみを対象とする。

一方で、システムの構成要素は、必ずしも人間が作ったものとは限らない。目的を達成するためには、天然資源など、人為的に作成されていないものも利用する。また、システムというと日本語では「情報システム」など、ハードウェアとソフトウェアを組み合わせたコンピュータや、それがなすネットワークを連想しがちであるが、それだけとは限らない。それを使うユーザ、操作するオペレータなどもシステムに含む。

他の文献によるシステムの定義を見てみる。国際的なシステムエンジニアリング団体INCOSEによる文献 [2]では、以下のように定義されている。

> System – An integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements （システム – 定義された目的を達成する、要素、サブシステム、部品などの統合された集まり。これらの要素には製品（ハードウェア、ソフトウェア、ファームウェア)、プロセス、人々、情報、技術、機材、サービス、その他の補助的要素が含まれる） (Appendix C)

この定義でも、システムとは「目的を達成するため」に構成されるものであると明記されている。また、システムの要素は、ハードウェアやソフトウェアだけでなく、人間、プロセス、機材といったものが含まれるという点も共通である。

システムや、システムの要素は互いに関連し、より大きなシステムをなす。図 2-1 は文献 [1]で示された階層的なシステムの構造である。システムは、必ず階層的に表現可能というわけではなく、分散して互いにやりとりするシステムも考えられる。システムを考える際、留意すべきことは、常に対象のシステム（System of Interest）がどの範囲までを含むのかを意識することである。これは、ステークホルダ間でシステムに関して議論する際に特に重要になる。

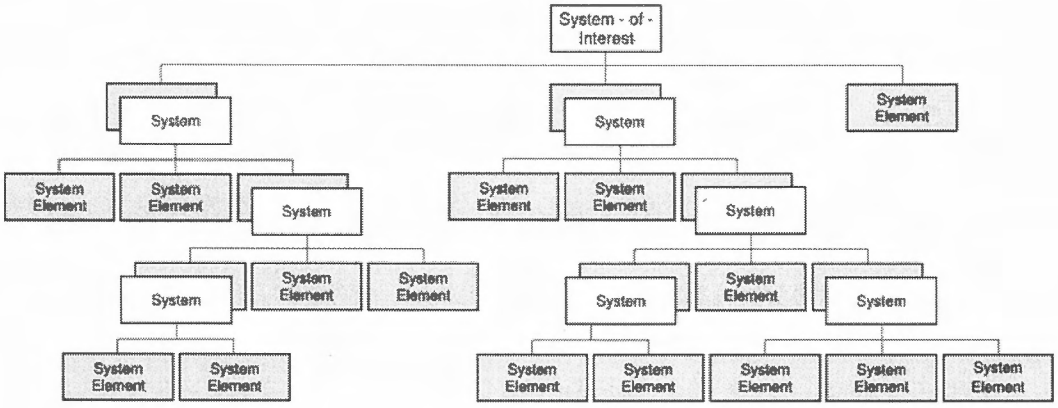

図 2-1 システムの構造（出典： [1] 5.2.2 System structure）

2.1.2. システムアシュランスとは何か

次に、システムアシュランスを解説する。一般名詞としてのアシュランス（assurance）は、確信・保証といった意味をもつ単語である[1]。保険（insurance）の一種という意味もあるが、システムアシュランスという用語では、前者の意味で使われる。Oxford Advanced Learner's Dictionary [3]における assurance の定義は以下である。

> a statement that something will certainly be true or will certainly happen, particularly when there has been doubt about it
> （何かが確かに正しい・確かに起こるという言明、特にそれに疑いがある場合の） (assurance, 用例 1)

システムアシュランスの文脈での「アシュランス」の定義は、システムアシュランスに関する国際標準群 ISO/IEC 15026 のうち、用語定義の部である ISO/IEC 15026-1 [4]にある。

> grounds for justified confidence that a claim has been or will be achieved （ある主張が達成される、または今後されるという正当な信用の根拠） (3.1.1 assurance)

この定義で重要な概念は、「主張」「根拠」「信用」の 3 つである。「主張」に「根拠」をつけることで「正当な信用」が得られる。なぜ正当な信用を得ているのか、システムの関係者に説明するためには、その根拠を明示し、議論・納得してもらうことが重要であることを示

[1] "assurance"の日本語表記には「アシュランス」と「アシュアランス」の 2 つがある。本論文では前者を採用する。

唆している。

システムアシュランスにおける「主張」は、ある「システム」が、望ましい特定の「性質」を持つ、という形で記される。性質の例としては、安全性（システムが誤作動して、人に危害を与えない）や、セキュリティ（システムが攻撃され、ダウンしない）がある。実際、システムアシュランスの分野は高度な安全性やセキュリティが求められるシステムを中心に発展してきた。

「性質」の具体的な例を挙げる。航空関係のシステムに限って、さまざまな性質を挙げたのが表 2-1 である。例えば飛行機システムであれば、飛行機に仮に問題が発生したとしても、墜落せず緊急着陸できるようにしてほしい、といった要望があるだろう。これは、安全性の要件の一つである。管制システムであれば、ネットワークを介して悪意ある者に侵入されて、飛行機の運航に異常をきたすようなことがあってはならない。これはセキュリティ要件の一つである。さらに、ウェブによる航空券予約システムであれば、予約したい人が画面操作でストレスを感じない、というユーザビリティが求められるだろう。あるいは、侵入者によって予約が不正に書き換えられないといったセキュリティも求められる。

このように、システムが持つべき性質は、システムによって多種多様であるし、性質は一つとは限らない。

表 2-1 アシュランス議論の例

対象システム	持つべき性質の一例
飛行機システム	安全性（飛行機に問題が発生しても、緊急着陸等の対策ができている）
管制システム	セキュリティ（管制システムが侵入者によって操作され、飛行機の運航に異常をきたさない）
航空券予約システム	ユーザビリティ（予約したい人が画面操作でストレスを感じない） セキュリティ（侵入者によって予約が不正に書き換えられない）

以上の「システムアシュランス」に関する検討を元に、本論文ではシステムアシュランス議論[2]を以下のように定める。

システムアシュランス議論　ある「システム」が望ましい特定の「性質」をもつということを、明確な証拠とともに主張し、ステークホルダ間でアシュランスを得る議論

すなわち、システムアシュランスを獲得するための手段として、システムのステークホル

[2] 日本語の「議論」に対応する英語には Argument や Discussion があるが、本論文では前者の意味で用いる。

ダ間で行われる議論である。

システムアシュランス議論は、「システム」と「そのシステムが持つべき性質」の２つをパラメータとして定めることによって、はじめて具体的に進めることが可能になる。さらに、「システム」も、より詳細に表現し、「システムが持つべき性質」も、より詳細に表現することで、深い議論が可能になる。このことは第３章で詳説する。

ここで重要なのは、「システム」と「システムの性質」という２つの概念があることと、それらを区別することである（図 2-2）。

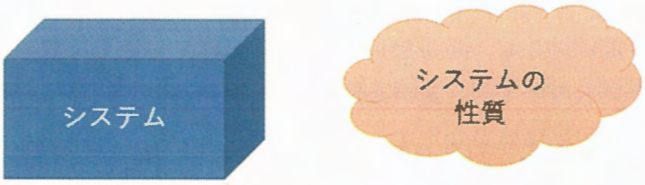

図 2-2 「システム」と「システムの性質」

2.1.3. システムアシュランス議論の必要性

なぜ、システムアシュランス議論が必要なのだろうか？　これに関して、システムアシュランスに関する文献 [5]に沿って解説する。この文献は、システムがセキュリティを持つことのアシュランスを中心に述べたものだが、必ずしもセキュリティに限定されない、システムアシュランスの一般的側面を説明している。少し長いが引用する。

> System engineering and system assurance are intimately related. To assure a system means to demonstrate that system engineering principles were correctly followed to meet the security goals. However, "good" system engineering as it is commonly understood does not guarantee that the resulting system will have the necessary level of system assurance. The need for providing additional guidance for system assurance is based on the rapid evolution of threats and changes in the operating environments of systems. The assurance of systems has usually been relegated to various processes as part of a broader systems engineering strategy.
> （システムエンジニアリングとシステムアシュランスは密接に関係する。システムをアシュアするとは、システムエンジニアリングの方針が正しくセキュリティの目標に適合することを証明すること、を意味する。しかし、「良い」システムエンジニアリングとして一般に知られるものは、結果としてできたシステムが必要なレベルのシステムアシュランスを持つことを保証しない。システムアシュランスのための補足的なガイダンスを提供する必要性は、システムに対する脅威の進化と、システムの利用環境の変化が急速に起きることに基づ

く。システムのアシュランスはしばしば、広範囲にわたるシステムエンジニアリング戦略の一部としての、さまざまなプロセスに追いやられてしまう。)
([5] Chapter 2.2.1)

・重要な点は以下である。

- 良いシステムエンジニアリングのプロセスが実施されたとしても、システムが持つべき性質に対して、必要なレベルのアシュランスが得られるとは限らない。
- アシュランスのガイダンスが必要なのは、システムに対する脅威が素早く進化し、システムの利用環境が変化するからである。

これらは、システムそのものだけに目を向けるのではなく、絶えず変化するシステムの周辺要素を考慮しないと、システムを維持管理できないことを示唆している。実際この文献ではこの後、以下の3つを継続的に実施することが、セキュリティ維持に必要であると述べている。

1. 適切なリスクアセスメント（リスク評価）
2. 適切なリスクアセスメントに基づくエンジニアリング
3. それらの活動が適切に実施されていることのアシュランス

リスクアセスメントとは、システムの外側にある脅威や懸念点を検討することである。この「システムの外側」を考えるという話は、本章で後述するシステムライフサイクルや、第5章で紹介するオープンシステム・ディペンダビリティという新しい信頼性の概念にも通ずる。

2.1.4. システムからシステムライフサイクルへ

ここで、システムライフサイクルを説明する。なぜなら、本論文では以下、システムライフサイクルに対するアシュランス議論を対象とするからである。

システムがある性質を持つことを議論するには、システムだけを対象にするのではなく、システムの周辺までを対象として広げていく必要があるというのが、近年の潮流である。そこで、「システムの周辺」を定義するために用いられるのが、システムライフサイクルの考え方である。

システムライフサイクルは、国際標準 ISO/IEC/IEEE 15288 [1]に定義されている。本標準は、システムライフサイクルの要素となる 30 のプロセスを定めたものである。

ここで、ISO/IEC/IEEE 15288 を簡単に説明する。この標準では、システムライフサイクルにおける作業の集まりを「プロセス」と呼ぶ。30 のプロセスが定義されており、これらのプロセスを自由に組み合わせることで1つのシステムライフサイクルを構築する。図 2-3 が 30 のプロセスである [1](5.6.1 Figure 4)。この並び順は時系列を意味しておらず、プロセスがいつ、どの順で呼び出されるかは、システムライフサイクル作成者が定義する。

また、図 2-4 に示すように、1つのプロセスは複数の「アクティビティ」によって構成さ

れ、１つのアクティビティは複数の「タスク」により構成される。その構造とは別に、１つのプロセスには複数の「アウトカム」が定められている。アウトカムとは、あるプロセスを正しく実装（具体化）した際に実現する状態や成果のことである。

また、プロセスは各組織に応じて、一定の基準に従って追加・修正して適用することが許容されている。これを「テーラリング」と呼ぶ。

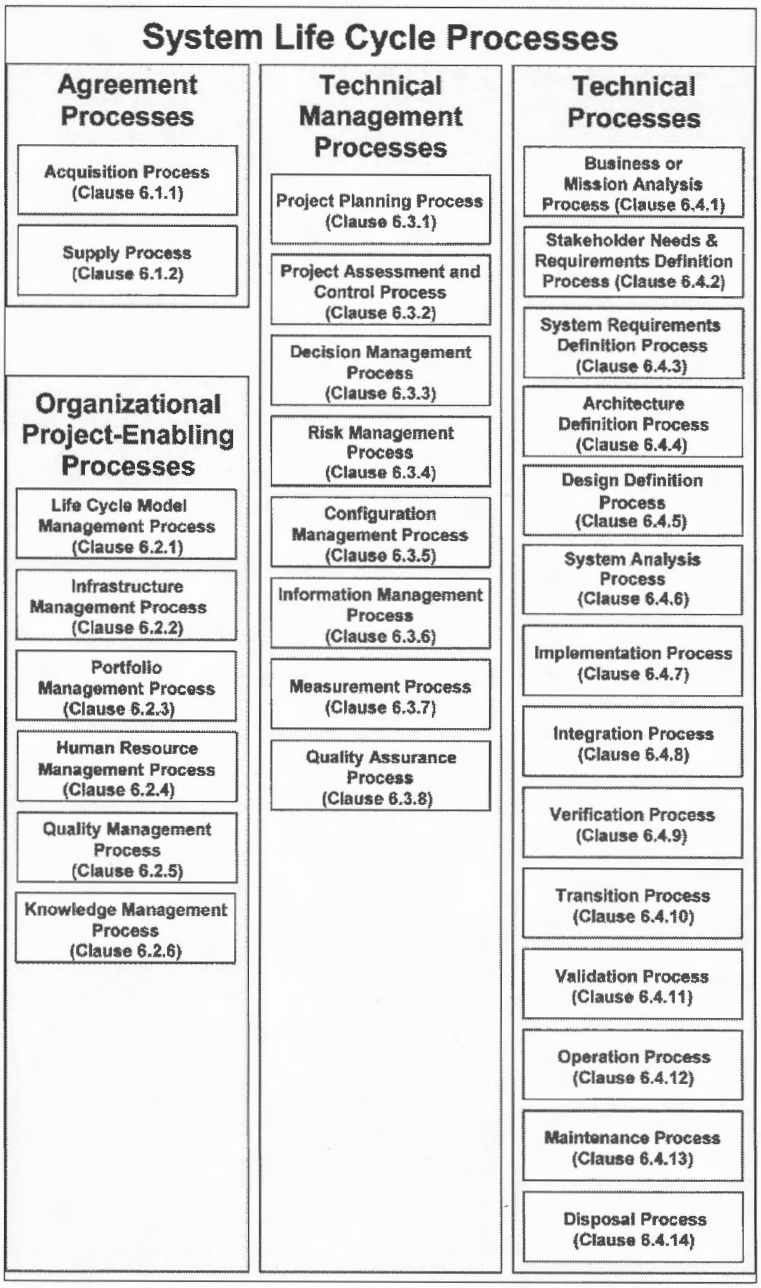

図 2-3　ISO/IEC/IEEE 15288 が定める 30 のプロセス（出典： [1] 5.6.1 Figure 4 – System life cycle processes）

本標準は、他の規格から参照・引用されて用いられることが想定されており、本標準を引用している規格が実際にいくつかある。以下はその例である。

- ISO/IEC 15026-4 [6]は、システムライフサイクルにおけるアシュランス獲得に必

要な作業と考慮点を、ISO/IEC/IEEE 15288 のプロセスごとに定めている。

- IEC 62853 [7]は、オープンシステムにおけるディペンダビリティ（信頼性）達成のための要件を、ISO/IEC/IEEE 15288 のプロセスごとに定めている。
- ISO/IEC/IEEE 24748-2 [8]は、ISO/IEC/IEEE 15288 を適用して個別のシステムライフサイクルを構築するためのガイドラインである。

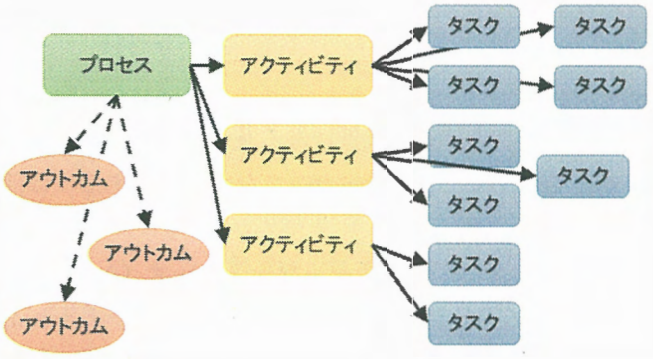

図 2-4 ISO/IEC/IEEE 15288 におけるプロセスの構造（著者作成）

2.2. アシュランスケース

2.2.1. アシュランスケースとは

システムアシュランス議論は、システムのステークホルダ間でなされるものである。議論でアシュランスを得るためには、ただ会議の場で資料を読み、それに基づいて議論をするだけでは不十分である。少なくとも、アシュランス議論で何が主張されたのか、それを示す証拠は何か、といった事柄を記録する必要がある。

アシュランスケースは、ステークホルダによるシステムアシュランス議論を記録した文書一式のことである[4]。アシュランスケースの最小限の構造と内容が、ISO/IEC 15026-2 [9]として国際標準化されている。この標準では、アシュランスケースは以下のように定義されている。

assurance case – reasoned, auditable artefact created that supports the contention

[4] アシュランスケースの「ケース」とは「場合」や「容器」の意味ではなく、判例・訴訟・弁論などを表す法律用語である。

that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)
アシュランスケース – 最上位の主張（または主張の集まり）は満たされるという主張全体を支えるためにつくられた、理由づけられ、監査可能なもの。主張を支える系統的な議論とその背景にある証拠および明らかな仮定を含む。
(3.1.3)

この定義の「系統的な議論」と「その背景にある証拠および明らかな仮定」という箇所に注目する。議論が構造化して記録され、議論の中でなされる各主張には前提条件や証拠があることが要求されている。

歴史的には、アシュランスケースはまずセーフティケース（Safety Case、安全ケース）として始まった [10]。システムの性質として、まず安全性が重要視されたためである。アシュランスケースは、セーフティケースを、安全性以外にも一般化したものである。

・なぜ、システムの安全性を示すためにセーフティケースが必要とされたのだろうか？ 文献 [11]に即して解説する。これは、システムを出荷する企業側と、そのシステムが安全であるかどうかの認証側（各国で構成される組織等）という、ふたつのステークホルダ間の関係の変化が原因である。この変化を、一般には規範的（prescriptive）な認証から、ゴール指向（Goal-oriented）の認証への変化と呼ぶ。

規範的な認証とは、認証する側がチェックすべき項目を提示し、認証を受ける側は、そのチェック項目を満たすようシステム・製品をつくる。これは、認証を受ける側は提示されたとおりに実施すればいいという簡便さがある一方、自由度が低い。また、認証する側は、その項目が実情に沿ったものであるかどうか絶えず見直さなければならず、負担が高い。

一方、ゴール指向の認証とは、認証する側は「システム・製品はこのような性質をもつ」「完成した結果、このような状態になっている」という「ゴール」のみを示し、認証を受ける側は、そのゴールが達成できるようシステムや製品をつくる。この方式は、認証を受ける側は、どのように実装するか考えなければならない負担がある一方、自由度が高い。また、本質的にものづくりは企業間の競争であり、実装こそが各社の競争力であると考えれば、自由度が高いのは自然なことである。また、認証する側は、ゴールを適切に決め、それを定期的に見直す必要性は変わらない一方、規範的な認証で細かい項目を定めるよりは負担が軽減されるという利点がある。

この、「認証する側はゴールを定める」「認証を受ける側は、ゴールを満たすことを示す」というコミュニケーションの表現手段として、セーフティケースが必要となったのである。

アシュランスケースは、当初は自然言語で記述された文書一式であった。しかし、ただ自然言語で記述されているだけでは、内容の理解に時間がかかり、ステークホルダ間のコミュニケーションに支障が生じるため、構造を表す図式法が提案されてきた。GSN [12]や CAE

[13]といったものが代表的である。本論文では以下、アシュランスケースの構築に際して、図式法を用いることを前提とする。

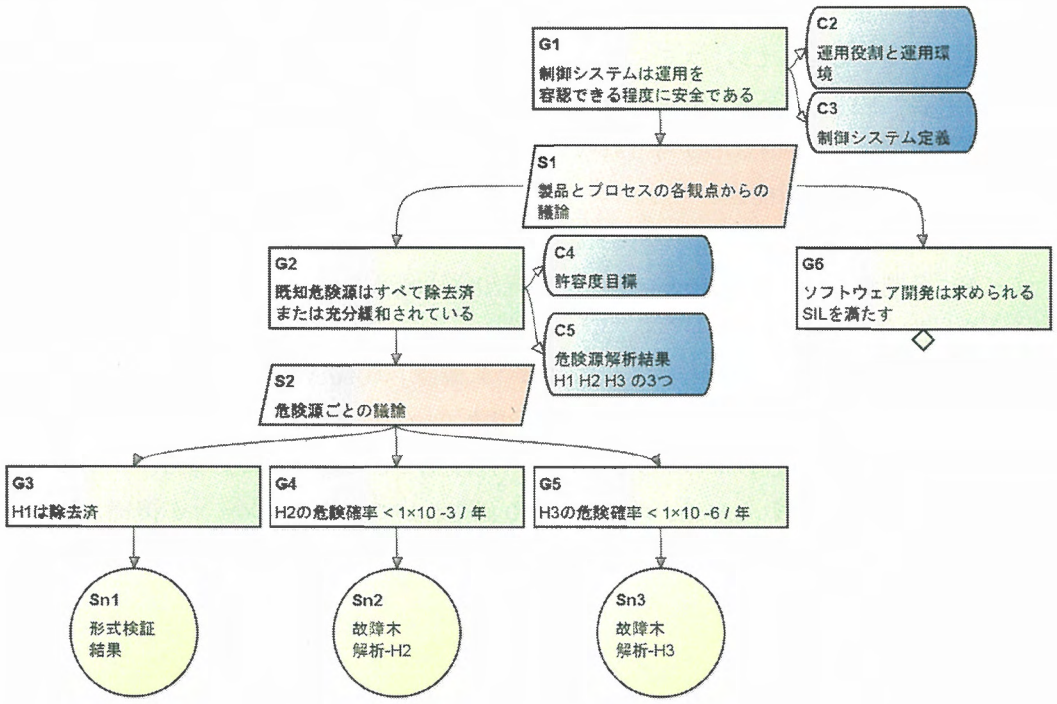

図 2-5 アシュランスケースの例（GSN 記法）

2.2.2. 図式によるアシュランスケース

ここで、文献 [14]の例をもとに、GSN 記法を用いたアシュランスケースを解説する。図 2-5 は「制御システムは安全性を持つ」ことを主張するアシュランスケースの例である。

GSN 記法では、主に 4 種類のノードを利用し、それらを矢印で接続することで構造を表現する。4 種類とは、「ゴール」（長方形）、「ストラテジー」（平行四辺形）、「ソリューション」（円）、「コンテキスト」（角なし長方形）である。上図ではそれぞれ色分けして緑、赤、黄、青で表現しているが、色は GSN 記法では規定されていない。

大まかにいえば、GSN 記法では、以下の手順でアシュランスケースを表記する。

1. 最も主張したいことをゴールとして書く（トップゴールと呼ぶ）
2. トップゴールをストラテジーによってさらに細かいゴール（サブゴールと呼ぶ）に分割する
3. サブゴールに、その主張が達成されることを示すソリューションを接続する
4. ゴール等で述べられることの前提となる定義をコンテキストとして付加する

図 2-5 に沿ってこのことを説明する。まず、トップゴール G1 は「制御システムは運用を容認できる程度に安全である」という主張である。ここでは、制御システムの「安全性」達

成の基準が、「運用を容認できる程度に安全」と定義されている。「運用を容認できる程度」の基準と度合いに対しての、ステークホルダ間の合意が、アシュランス議論のために重要である。単に「制御システムは安全性を持つ」という記述のままでは、ステークホルダによって「安全性」の基準が異なるかもしれない。また、基準が一致しても、度合いが一致せず、議論がかみ合わない可能性がある。

次に、このゴールをストラテジーS1「製品とプロセスの各観点からの議論」で2つのサブゴールに分割する。それぞれ、ゴール G2「既知危険源はすべて除去済または充分緩和されている」とゴール G6「ソフトウェア開発は求められる SIL を満たす」である。後者のゴール G6 は、下に菱形が付されている。これは「未確認」(Undeveloped) と呼ばれる記号で、このゴールが達成されるかどうかはまだ確認できていないことを示す。

前者ゴール G2 は、さらにストラテジーS2「危険源ごとの議論」によって、3つのサブゴールに分割される。これらには、ゴール達成の証拠としてソリューションが接続されている。それぞれ、ゴール G3「H1 は除去済」に対してはソリューション Sn1「形式検証結果」、ゴール G4「H2 の危険確率＜1×10^{-3}/年」に対してはソリューション Sn2「故障木解析-H2」、ゴール G5「H3 の危険確率＜1×10^{-6}/年」に対してはソリューション Sn3「故障木解析-H3」である。

最後に、「コンテキスト」を説明する。ゴール G1 は「制御システムは運用を容認できる程度に安全である」という主張である。この主張が意味をなすためには、例えば制御システムとはどんなシステムなのか、その運用とはどんなものなのかに関して、議論を行うステークホルダが合意しなければならない。そこで、コンテキスト C2「運用役割と運用環境」とコンテキスト C3「制御システム定義」が付加されている。これらは、実際に運用や制御システムが定められた文書のラベル（あるいは、文書へのリンク）だと考えればよい。また、G2「既知危険源はすべて除去済または充分緩和されている」にも、コンテキスト C4「許容度目標」とコンテキスト C5「危険源解析結果」が付されている。これらは、「既知危険源とは何か」「充分緩和されているとはどういうことか」といったゴールの文言への疑問を説明するものである。

GSN 記法にはその他のノードの定義もあるが、本論文の主題「アシュランス議論のためのオントロジー」のために必須ではないので割愛する。次章で詳述するアシュランス議論のためのオントロジーは、上記4つのノードで言えば「コンテキストとは何か」という問題を解決するために必要なものである。

2.2.3. アシュランスケース構築における問題

システムアシュランス議論の記録法として、図式によるアシュランスケースの構築を紹介した。GSN や CAE といった図式法によって、アシュランスケースはステークホルダ間の議論を促進する役割を果たしたのであった。一方、図式法によるアシュランスケース構築にも問題があることが明らかになってきた。それは、アシュランスケースの整合性を担保しつ

つ維持・管理していくことの困難さである。この問題を、文献 [15]の記述に即して解説する。

システムの記述とシステムの性質の記述が巨大で複雑になるにつれ、アシュランスケースはしばしば、巨大で複雑な文書群となる。前章で紹介した図 2-5 を例にすると、「制御システムは運用を容認できる程度に安全である」という主張の達成を議論する場合、「制御システム」がより厳密に定義され、「運用を容認できる程度に安全である」という性質がより厳密に定義されるにつれ、アシュランスケースは図 2-5 よりもはるかに大きなものになる。

一方で、たとえ巨大で複雑になったとしても、そのアシュランスケースが整合性をもつことは不可欠である。なぜなら、ほんのわずかな整合性の破綻が、アシュランスケース全体を無意味にするからである。

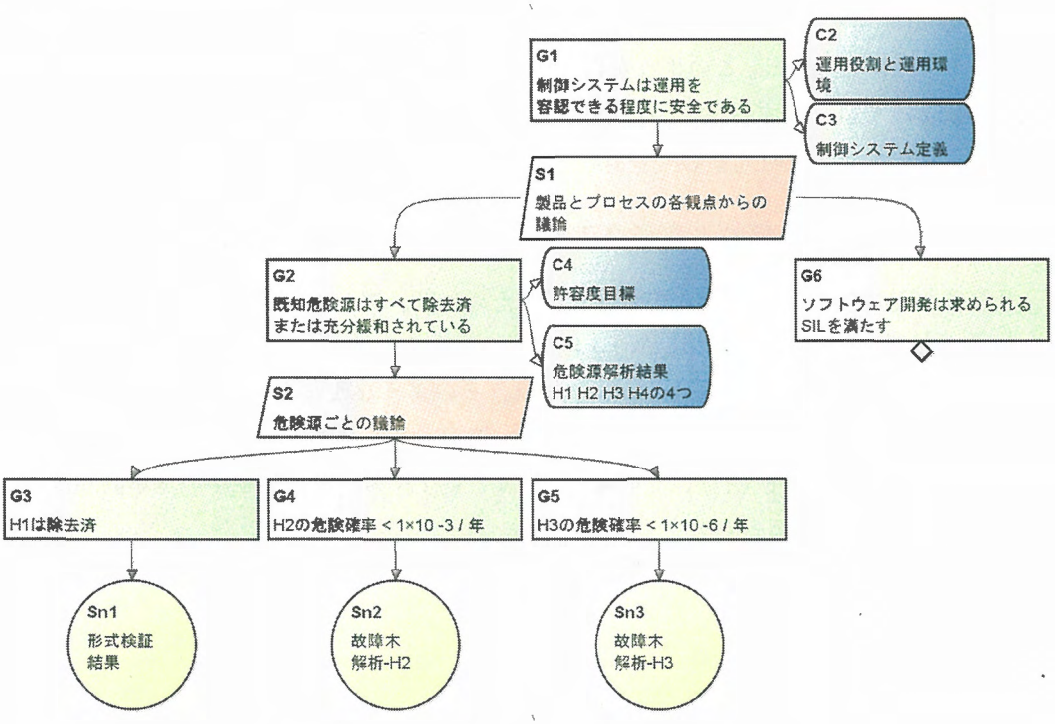

図 2-6 整合性が破綻したアシュランスケース

引き続き図 2-5 を例にとる。ストラテジーS2「危険源ごとの議論」では、危険源は H1、H2、H3 の 3 つであった。しかし、危険源解析が再びなされ、危険源として H4 が追加された場合、図 2-5 のアシュランスケースの整合性は破綻する（図 2-6）。すなわち、コンテキスト C5「危険源解析結果」と、ストラテジーS2「危険源ごとの議論」とが不整合になる。なぜなら、危険源は H1 から H4 までの 4 つ存在するにもかかわらず、S2「危険源ごとの議論」では、危険源 H4 に対する議論がなされていないからである。整合性（アシュランスケース内での論理的な正しさ）が破綻したアシュランスケースに対して、その妥当性（アシュランスケース全体を、外部の諸概念と照らし合わせたときの正しさ）を議論することは無意

味である。

図式によるアシュランスケース記述では、上記のような不整合を発見しづらい場合がある。すなわち、コンテキスト C5 の文言をよく読み、S2 と比較すれば、不整合を発見できる。しかし、アシュランスケースの図式法は、各ノードの中に記述すべき文言の様式を特に規定しない。図 2-5 と図 2-6 はともに、正しく GSN 記法に従って記されたアシュランスケースであるし、例えば、C5 が単に「危険源解析結果」とだけ記されていたとしても、正しく GSN 記法に従って記されているといえるのである。記法が定義されていたとしても、記述において重要な部分は、アシュランスケースを構築するステークホルダに委ねられている。

このように、アシュランスケースの整合性を担保しつつ維持・管理し、意味あるものとしていくことは困難を伴う。このような整合性の検査は、人間によるレビューだけではなく、計算機によって自動化するほうが効果的であるという着想から、アシュランスケース構築におけるツール支援が研究されている。

2.2.4. 形式理論と証明による形式アシュランスケース

計算機による整合性の自動検査を実現するためには、アシュランスケースの数理的モデルを構築し、それに基づいて自動検査を実施するという方式が考えられる。形式アシュランスケース（formal assurance case） [15] [16]は、そのような数理的モデルに基づくアシュランスケース表現として提唱されている。これは、アシュランスケースを形式理論（formal theory）と、その理論での証明として定義している。以下では、数理論理学の基本的知識 [17] [18]を前提に話を進める。

形式理論における諸概念と、アシュランスケースの GSN 記法における諸概念の対応を [15]に基づいて整理したのが表 2-2 である。

表 2-2 形式理論とアシュランスケースの諸概念の対応

形式理論の概念	アシュランスケース（GSN 記法）の概念
命題	ゴール
推論規則	ストラテジー
前提から推論規則によって結論を導くこと	ゴールをストラテジーによってサブゴールに分割すること
ある命題を公理と定めること	ソリューションによってゴールが成り立つと定めること
言語による公理、命題、推論規則の定義とそれへの参照	コンテキスト

ここで注意しておきたい点が２つある。１つは、公理に対する考え方である。自然数に対する形式理論のように、一般に形式理論を適用する場合、公理とはペアノの公理のように「誰もが正しいと認める命題」である。それに対して、具体的なアシュランスケースを形式

理論の一例としてとらえる場合、公理とは、誰もが正しいと認める命題にはならない。

再び図 2-5 に即して説明する。このアシュランスケースにおいて、ゴール G3「H1 は除去済」は、ソリューション Sn1「形式検証結果」が証拠であると示されている。これは、

- 「H1 は除去済」という命題が、この公理系における公理であるという事実
- その事実に対するラベルとして「形式検証結果」という名前を付ける

ということを示している。「H1 は除去済」という命題は、世間一般に正しいと認められる命題ではないが、あくまでもこの公理系における公理として定められる。このアシュランスケースが妥当であるかどうかの議論は、この公理系の妥当性に帰着する。

注意しておきたい点の 2 つ目は、コンテキストの定式化である。GSN 記法などの図式によるアシュランスケース記述では、議論が基づくコンテキストが変更されたとしても、議論を修正する必要性に気づかない可能性があった。しかし、形式アシュランスケースにおいては、コンテキストは「命題や推論規則を表現するための言語」および、その定義への参照であると考える。これは、コンテキストにおいて定義されていない語彙は、ゴールやストラテジーに記述できないことを意味する。この制約によって、議論が基づくコンテキストが変更されたときに、議論を修正すべきかどうかの検査が可能になる。この検査の自動化を実現したのが、次節で述べるプログラミング言語 Agda による実装である。

2.2.5. Agda による形式アシュランスケースの実装

形式アシュランスケースは、プログラミング言語 Agda [19]によって FACIA（Formal Assurance Case in Agda）として実装されている。Agda は構成的型理論に基づく汎用的な関数プログラミング言語 [44]であり、定理証明器でもある。依存型（dependent type）と呼ばれる型によって、直観主義高階述語論理に相当する高い表現力を持つため、さまざまな数学的概念を形式化するツールとして用いることができる。

Agda[6]は、プログラミング言語 Haskell [20]で実装されている。Haskell の処理系 GHC が動作する環境すなわち Windows, Mac, Linux 等で動作する。また、エディタ Emacs [21]上でインタラクティブな開発を実施することができる。Agda を用いることで、以下のアシュランスケース構築における問題が解決した（表 2-3）。また、図 2-5 の GSN 記法によるアシュランスケースを、Emacs 上の Agda 開発環境で整合性検査している例が図 2-7 である。アシュランスケースに記された文言は、プログラミング言語 Agda 上の型や関数として定義され、アシュランスケースの整合性検査は、Agda の型検査に帰着する。これらの詳細は文献 [15]に詳しい。

---

[6] プログラミング言語とその処理系は別のものであるが、本論文では通例にならい、プログラミング言語 Agda の処理系も Agda と呼ぶ。

表 2-3 アシュランスケース構築における課題の Agda による解決

アシュランスケース構築における課題	Agda における解決・実現法
整合性検査	Agda コードの型検査
トレーサビリティ	Emacs 上での操作で、Agda コードの定義に移動する
構造化	Agda のモジュールシステム
テンプレートに基づく開発	Agda のパラメタ付きモジュール

アシュランスケースの拡張構文である D-Case においては、D-Case in Agda が実装され、GSN に準じた図式法でアシュランスケースを描画するツール D-Case Editor と、相互に変換することも可能となった [15]。これは、プログラミング言語 Agda の読解や記述が困難なステークホルダに対しても、形式アシュランスケースを用いたコミュニケーションを可能にした。

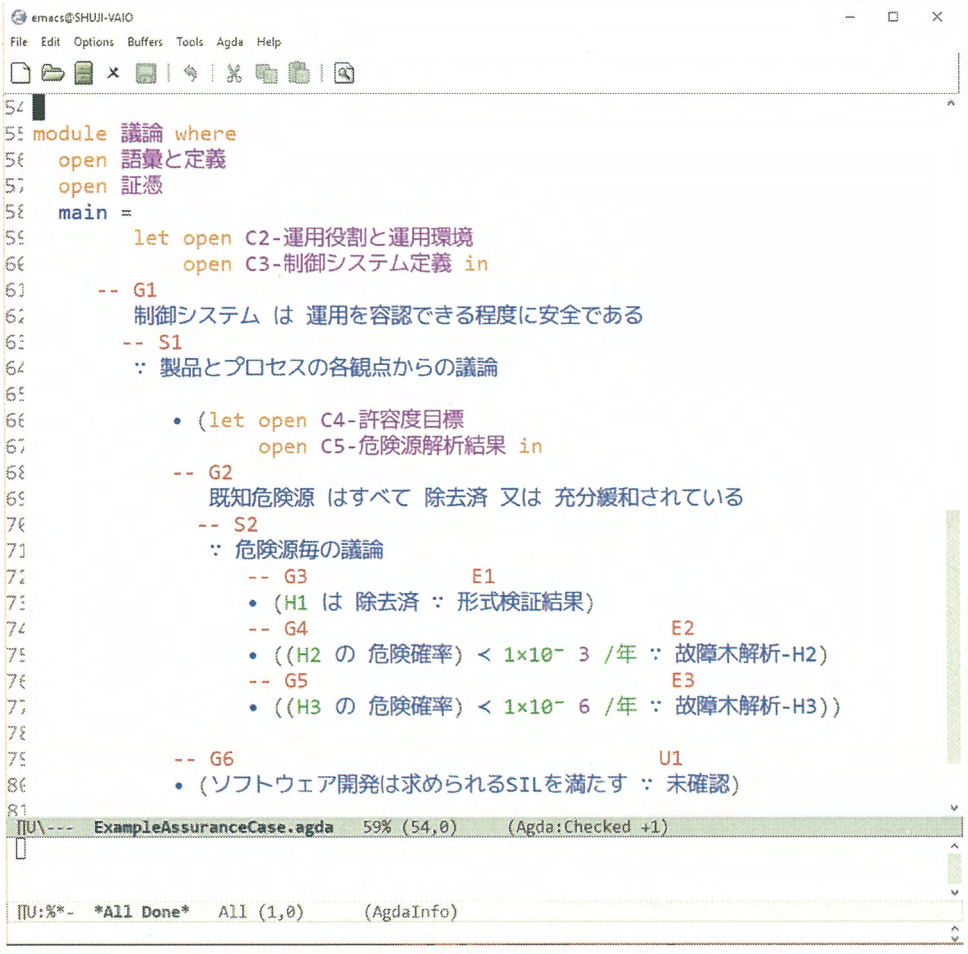

図 2-7 Emacs 上の Agda 開発環境による形式アシュランスケース

自然言語で記されたアシュランスケースが図式化され、形式アシュランスケースと Agda による実装によって機械処理可能になった、という時間の経過は、プログラミング言語のそれと類似している。すなわち、以下のような対応がある（表 2-4）。

表 2-4 プログラミング言語とアシュランスケースの発展経過の類似

	プログラミング言語	アシュランスケース
初期	アセンブラなどの低級言語による開発	自然言語によるアシュランスケース記述
課題 1	読解の困難	
中期	フローチャートによる構造化の図式	GSN、CAE 等による構造化の図式
課題 2	機械処理の困難	
後期 (現在)	C 言語などの高級言語による開発	Agda 言語による形式アシュランスケース記述

初期のプログラミングにおいては、機械語に近いアセンブラのような低級言語による開発が主流であった。しかし、このような低級言語で記されたプログラムは読解が困難であり、フローチャートのような構造化された図式法が利用された。しかし、フローチャート自体は機械処理できるものではない。現在は言うまでもなく、C 言語など抽象度の高い高級言語によるプログラミングが主流である。Java などのオブジェクト指向プログラミング言語や、Haskell などの関数型言語など、さまざまな形式の高級言語がある。

この経過は、アシュランスケース構築の現在までの経緯に類似している。すなわち、自然言語で記されたアシュランスケースの読解の困難さから、GSN、CAE 等の図式法が生まれた。しかし、図式の構造の機械処理は困難である。形式アシュランスケースでは、図式ではなく形式言語を対象とすることによって、構造の機械処理が実現されている。

プログラミング言語において、高級言語が一般化したことは、アシュランスケースにおいても、形式アシュランスケースが一般化していくことを示唆する。さらに、C 言語以外にさまざまな高級言語が考案され、プログラミング手法が発展していることは、形式アシュランスケースにおいても、Agda による形式アシュランスケースに限らず、さまざまな発展の余地があることを示すだろう。

3. 課題：アシュランスケースにおけるオントロジーの重要性

本章では、前章で紹介したアシュランスケース構築における問題点として、オントロジーの重要性を述べる。まず、アシュランスケースにおけるオントロジー一般の問題を述べる。次に、システムライフサイクルに対するアシュランス議論における、システムライフサイクルプロセスのオントロジー構築の問題を説明する。

3.1. アシュランスケースにおけるオントロジー

. アシュランスケースを用いたアシュランス議論は、さまざまなステークホルダが関与して行われるものである。ステークホルダ間での議論を円滑に進めるためには、以下の手順を踏んで議論を進めることが重要である。

1. 議論の前提となるシステムやシステムの性質を書き下すこと
2. 書き下した内容に関して、ステークホルダで合意すること
3. その上でシステムアシュランス議論を実施すること

システムやシステムの性質を書き下すためには、さまざまな語彙とその基本的性質を定める必要がある。この「語彙とその基本的性質」を、本論文では「オントロジー」と呼ぶ。オントロジーは、システムアシュランス議論のさまざまな段階における円滑なコミュニケーションの礎を与える。

オントロジーを構築することは大変な労力を要するし、一般の文書の維持管理と同様、その後の維持管理にも困難を伴う。プログラミング言語 Agda による形式アシュランスケースの実装は、そのような維持管理を汎用のプログラミング技術を利用して軽減できることを示した。これは、様々なシステムアシュランス議論をより厳密に実施するための土台が整ったことを意味する。

この結果、課題として残されたのは「議論に適したオントロジーをどのように構築するか」ということである。「オントロジー」は大きく次の２つに分けられる。

1. 「システム」のオントロジー
2. 「(システムが持つべき) 性質」のオントロジー

である。

本論文は、１つ目「システム」のオントロジーの構築法の研究である。ここで、「システム」とは、システムそのものだけでなく、広くシステムの周辺にある他のシステムや、環境、人なども含む。すなわち、2.1.4 節でも述べたように、システムがある望ましい性質を持つことの確信を得るには、システムライフサイクルを定め、それらが望ましい性質を持つことを議論する必要がある。システムライフサイクルは、システムライフサイクルプロセスから

なる。そのため、どのようにシステムライフサイクルプロセスをオントロジーとして記述するかが問題になる。

3.2. システムライフサイクルプロセスのオントロジー構築における課題

システムライフサイクルプロセスのオントロジー構築にあたり、本論文では第 1 章で紹介した国際標準 ISO/IEC/IEEE 15288 [1]に基づくこととする。この標準はシステムライフサイクルプロセスの一般的枠組を与えるもので、広く受け入れられている。しかし、この標準は具体的なシステムライフサイクルプロセスの記述法を与えるものではないので、具体的な記述法は個々で検討する必要がある。本節では、具体的な記述法検討に際しての課題を詳説する。

ISO/IEC/IEEE 15288 は、プロセス、アクティビティ、タスクという 3 層構造を持つのであった。しかし、プロセスの各アクティビティ、各タスクをどのように記述すればよいかは、必ずしも明らかではない。例えばタスクは、用語定義の項では以下のように定められている。

> "required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a process"（プロセスの 1 つ以上のアウトカムの達成に貢献することを意図して、要求、推薦もしくは許可された動作）([1] 4.1.50)

これは、タスクがどのようなものかを定めている一方、実際にタスクをどのように記述していけばよいかは明らかでない。

具体的なプロセスの 1 つのアクティビティを取り上げ、タスクの記述を概観し、タスクの記述法が自明でないことを示す。完成したシステムを操作するプロセスを定めた Operation Process の最初のアクティビティを紹介する。

a) **Prepare for operation.** This activity consists of the following tasks:

1) Define an operation strategy.

2) Identify system constraints from operation to be incorporated in the system requirements, architecture, or design.

3) Identify and plan for the necessary enabling systems or services needed to support operation.

4) Obtain or acquire access to the enabling systems or services to be used.

5) Identify or define training and qualification requirements for personnel needed for system operation.

6) Assign trained, qualified personnel to be operators.

([1] 6.4.12.3 より抜粋。NOTE 等、タスクの詳細な説明は省略)

このアクティビティは、「Prepare for operation」という名前からわかるように、オペレーションの準備に際して必要なタスクを示している。例えば 1 つ目を和訳すると「オペレーションの戦略を定義せよ」となる。しかし、具体的なシステムのライフサイクルプロセスで解釈した際に、どのような業務が「オペレーションの戦略を定義」することになるかは、何も述べていない。

これは、ISO/IEC/IEEE 15288 は特定のシステムに対して記述しておらず、一般のシステムに対して抽象的なレベルで記述しているからである。具体的なシステムにおいて、タスクが示した「仕様」をどのように「実装」するか、またその実装がどのように記述されるかは、標準を利用する側に委ねられている。

以上のように、タスクの記述法は自明なものではなく、システムライフサイクルプロセスのオントロジーは、ISO/IEC/IEEE 15288 のみから系統的に構築することは難しい。そこで、ISO/IEC/IEEE 15288 に関連する規格群を援用することを以下で検討する。

2.1.4 節で紹介した、ISO/IEC/IEEE 15288 の適用ガイドラインである ISO/IEC/IEEE 24748-2 [8]には、記述方式に関する記載はない。「プロセス」とは入力と出力があることなど、プロセスという概念はどのようなものかの説明はあるものの、その概念をどう記述するかは、標準を利用する側に委ねられている。

国際標準 ISO/IEC/IEEE 15289 [22]は ISO/IEC/IEEE 15288 の各プロセスにおける入出力となる情報を定める規格であるが、システムライフサイクルプロセスのオントロジーを構築

する具体的な方法までは定めていない。"7.5 Procedure – generic content" という節では、入出力となる情報の種類として「Procedure（手続き）」を挙げ、それらに含むべきもののひとつとして "Ordered description of steps to be taken by each participant"（各参加者によって実施される、順序づけられた手順の記述）を挙げているが、その記述に何を含むべきかは、明記されていない。

このように、記述法を国際標準が何も示さない理由は、以下の 2 つが考えられる。

1. 「プロセス」そのものと、「プロセスの記述」は別。これらの標準はあくまでも「プロセス」を定めるものであって、「プロセスの記述」を定めるものではない。
2. あるプロセスが適切に実施されているかどうかを確認する手法は、プロセスの記述を確認すること以外にもある。例えば、「プロセスの入出力が適切であること」を確認することで、プロセスが適切に実施されていることを確認する手法がある。

1 は、プロセスをホワイトボックスだと考え、その中身を記述しようとする視点に立つ。2 は、プロセスをブラックボックスだと考え、その中身は記述せず、外延的な振る舞いを確認する視点に立つ。これら 2 つの視点は、どちらも必要である。そこで、前者の立場で、プロセス・アクティビティ・タスクとして、どのような事項を記述するかの枠組みを作る必要がある。

3.3. 事例：ライフサイクルプロセス適合性議論におけるオントロジー

ここまで、アシュランスケース構築におけるオントロジーの問題を概観し、特にシステムライフサイクルプロセスのオントロジー構築法を定める重要性を説明した。ここで、アシュランス議論におけるオントロジーの重要性を示す事例を紹介する。これは、安全性に関する国際標準に適合したソフトウェアライフサイクルの認証に関して、著者らが企業に聞き取りを行い、それに基づいて、アシュランスケースの適用可能性を検討したものである（発表リスト 3）。

図 3-1 は、あるソフトウェア開発企業 X が、国際標準を解釈して自社のソフトウェアライフサイクルを改善する事例を図示したものである。以下、順に説明する。本文中の丸数字と SLC1 などのラベルは図 3-1 に対応する。

① X 社は、自社のソフトウェアライフサイクル SLC1 が、安全性標準 STD に適合していることの認証を申請することとなった。

② X 社は、申請前に、自社のライフサイクル SLC1 が標準 STD に適合することを主張するアシュランス議論を行い、アシュランスケース A1 として記録する。

③ そのためには、STD を SLC1 の文脈で解釈した I1 が必要である。これもアシュランスケース A1 の一部として記録されている。

残念ながら、最初の認証申請は却下されてしまう。このときなぜ却下されたのかの理由は通知されず、自ら探さなければならない（却下の理由を通知することは、利益相反にあたる

ため)。

④ アシュランスケース A1 が再検討され、2つの原因が発見される。この原因を修復するには、標準の解釈を修正する必要がある。

⑤ 標準 STD の解釈を I1 から I2 に修正し、ライフサイクルを SLC1 から SLC2 に変更する。

⑥ SLC2 が解釈 I2 を満たすことをアシュランスケース A2 として記録する。

このシナリオは 2 回目の認証申請の合格（認証）によって終了する。

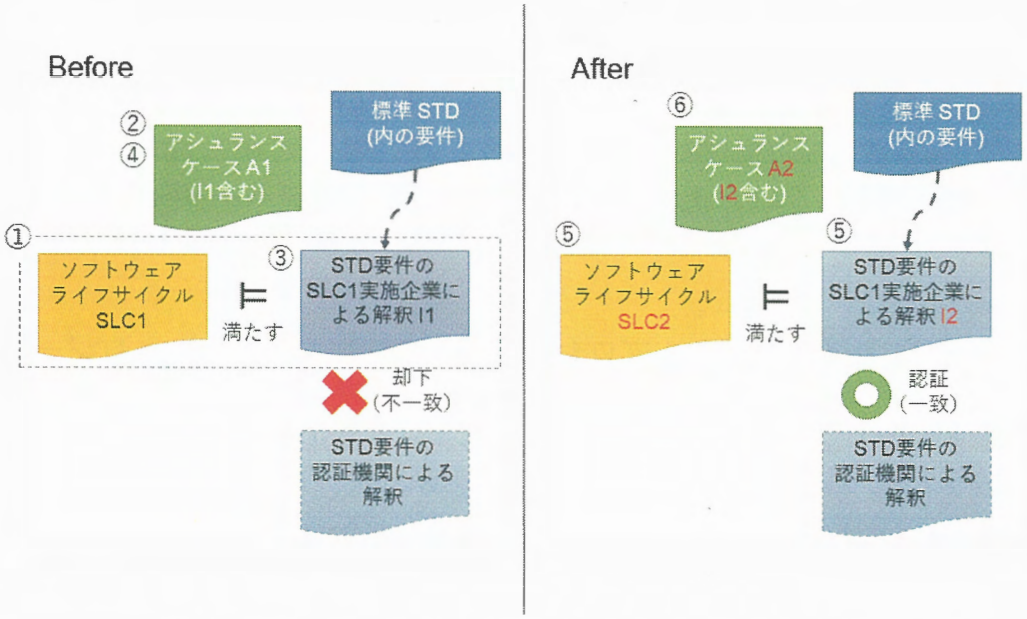

図 3-1 標準に適合したソフトウェアライフサイクルと、その解釈の関係

この事例は、アシュランスケース記述によってオントロジーを明確に示しておくことで、標準への適合性認証が円滑に進むことを示すものである。オントロジーを明らかにすべき対象は、要求を定めた標準 STD であり、それに基づいて構築されたソフトウェアライフサイクルの記述 SLC1, SLC2、そして STD を SLC1, SLC2 の文脈で解釈した I1, I2 である。これらの記述が、どのような語彙で記され、語彙どうしがどのように関係するかを明らかにする過程で、より厳密なアシュランス議論ができ、その結果はアシュランスケースとして記録される。

特に、必ずしも明文化されない「解釈」のオントロジーを明らかにすべきことは、注目すべき点である。標準に記載されている要件の適合性に関して議論するには、必ず I1 や I2 のような解釈が必要である。なぜなら、要件は各企業の具体的な文脈に沿って書かれておらず、自社のライフサイクルが安全性の要件を満たすことを主張するためには、要件を具体的な文脈（すなわち、自社製品や開発プロセスを定めるオントロジー）に沿って言い換える必要があるためである。

このような「解釈」を円滑に進めるためには、これまで述べたシステムライフサイクル（この場合は特に、ソフトウェアライフサイクル）のオントロジー記述の枠組みがあることが望ましい。その枠組みとして次章で提案するのが、6W1H モデルである。

4. システムライフサイクルプロセスのオントロジー構築法としての 6W1H モデル

本章では、システムアシュランス議論におけるオントロジー構築法として「6W1H モデル」を提案する。ISO/IEC/IEEE 15288 [1]に基づいてシステムライフサイクルプロセスを記述することで、より効果的なシステムアシュランス議論が可能になる。一方で、ISO/IEC/IEEE 15288 は、システムライフサイクルプロセスを「プロセス」「アクティビティ」「タスク」という 3 層構造で定めているものの、具体的なひとつひとつの作業（アクション）の記述法は定めていない。

そこで本章では、システムアシュランス議論のための、システムライフサイクルプロセスのオントロジー構築法として、6W1H モデルを用いた手法（発表リスト 1）を提案する。これによって、IEC 62853 [7]が提供するディペンダビリティ議論のような、ISO/IEC/IEEE 15288 に基づいたシステムアシュランス議論の構築が促進される。

4.1. 「アクション記述の枠組み」としての 6W1H モデル

6W1H モデルとは、「6 つの W（Who、What、Whom、Where、When、Why）で表現される人間の作業（以下、アクション）」をノードとする木である。「6W1H」とは、Who, What, Whom, Where, When, Why, How の略で、すなわち「誰が、何を（どうした）、誰に、どこで、いつ、なぜ、どのように」を意味する。これは、ジャーナリズムにおいて、事象記述のために重要な要素としてよく知られる 5W1H に「Whom」を追加したものである。

6W1H モデルでは、6W と 1H を分けて考える。前述のように、まず 6 つの W によってひとつのアクションを記述する。次に、ひとつのアクションを複数のアクションによって、より詳細に記述してゆく。この一対他の関係が 1H、すなわち How である。一般に、「ある 1 つのアクション」は、複数のアクションによって詳細に表現でき、木構造をなす。これは、システム開発における「仕様」と「実装」の関係に似ている。すなわち、ある 1 つのアクションとして表現された「仕様」が、複数の詳細なアクションによって「実装」される。

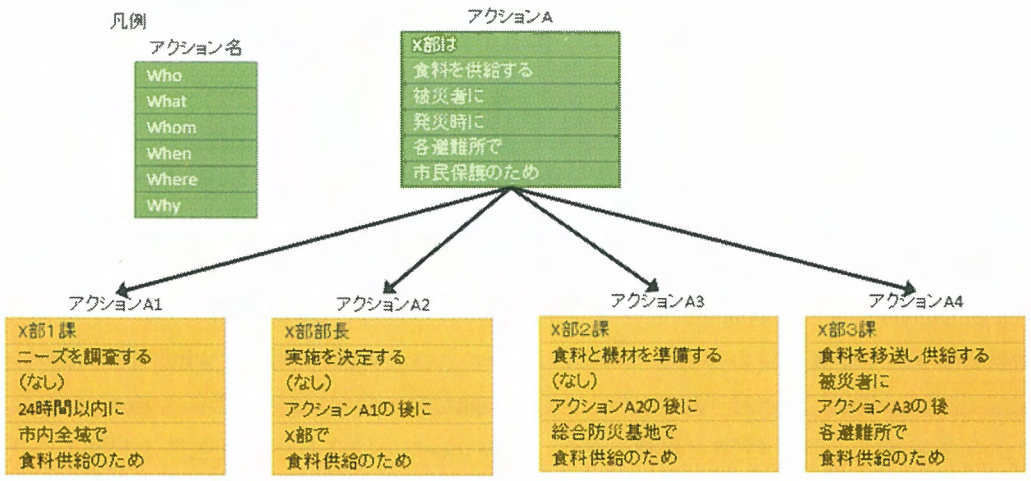

図 4-1 発災時の食料供給業務を 6W1H モデルで表現した例

図 4-1 は 6W1H モデルの例である。6W1H モデルと、その補助的な図式法を用いて、発災時の食料供給業務を示した。最上位のアクションで記された 6W を文章にすると「市民保護のため（Why）、X 部は（Who）発災時に（When）各避難所で（Where）被災者に対して（Whom）食料を供給する（What）。」となる。このアクションは、より詳細な記述を持つ 4 つのアクションに分割される。各アクションの「What」は、「ニーズを調査する」「実施を決定する」「食料と機材を準備する」「食料を移送し供給する」である。これら 4 つのアクションは、システムのステークホルダが最も下位のアクションを実行できると合意できるまで、繰り返して詳細化できる。例えば、アクション A1「食料供給のため、X 部 1 課は 24 時間以内に市内全域でニーズを調査する」は、市内のどこを調査するかによって分割することができる。

4.2. 関連研究

6W1H モデルのように、人間の動作を記述する枠組みとして、5W1H[7]や、それを一部改変したものを用いる研究や開発手法はいくつかある。また、システムエンジニアリングの分野にはさまざまなモデリングの手法があり、それらをシステムアシュランス議論のためのオントロジー構築に利用することもできる。本節では、それら関連研究を概観する。

[7] なお、欧米では"5W1H"ではなく"5Ws"という表記を用いることが多い。

4.2.1. 5W1H 等を用いたモデリング

5W1H、6W1H そのものは特定の研究分野を形成していないが、さまざまな分野において、これらを利用した研究や開発手法がある。これらと比較した際の本研究の特色は、「6W は木構造をなし、How とは木の親子関係を表現したものである」と考える点である。

文献 [23]は、システム開発プロジェクトの各フェーズで、5W4H を用いてプロジェクト管理を行う日本企業向けの手引きである。5W4H とは、What（何を）Why（何のために）Who（誰が）When（いつ）Where（どこで）に加えて、How（どのように）How many（どのような品質、工期、目標を目指して）、How much（どのような生産性を目指して）、Humanware（人間力を持って）を指す。特に Humanware を加えていることに特徴がある。

文献 [24]は、システムエンジニアリングにおけるビジネスミッションを定めるために、6W1H を用いて曖昧さをなくす手法を紹介している。この 6W1H は本稿と同一のものであるが、異なる順序で Who, What, When, Why, How, Which, Whom と記されている。How とは「エンジニアリング」であるとし、Who, What といった 6W がなす仕様に対する実装を示唆しているが、それらが階層構造をもつとは述べていない。

文献 [25]は、ビジネス上の課題分析に 5W1H を用いる手法の解説書である。経営大学院などで指導される多数の分析手法を理解し、適切に使い分けることは困難なので、シンプルな 5W1H だけを基本として、それを応用することを提案する。特色は、常に 5W1H の項目をすべて使うのではなく、状況に応じて抜粋して利用することの提案である。例えば、第 3 章では「Why-What-How」の 3 つを利用して説明の骨組みを作る手法を紹介している。また、第 5 章では 3W1H による問題解決のステップとして、①What（何を解決するのか）？②Where（どこが悪いのか）？③Why（なぜ起こるのか）？④How（どうするのか）？という手順を紹介している。

文献 [26]は、ビッグデータの解析と可視化に 5W1H を利用する研究である。5Ws Model という名称で、データとは何か（What）、どこから来たデータか（Where）、いつ発生したデータか（When）、誰が受け取ったデータか（Who）、なぜそのデータは発生したか（Why）、どうやってデータは運ばれたか（How）という 6 つの視点でデータを分類する。人間の動作ではなく、データをこのような 6 項目で分類し、さまざまなデータベースに対して統一的視点を与える点に特色がある。

文献 [27]は、法科学のひとつであるデジタルフォレンシクス解析に、6W1H を用いた質問を利用する研究である。さまざまな法的証拠を収集する過程で複雑になりがちな個々の作業によって本来の目的を見失うことがないよう、6W1H による質問で全体図を描くという手法である。この「全体図を描く」という目的は、文献 [24]のミッション解析や、次章で述べる「システムの全体像を把握する」（5.2.1）にも共通する。

文献 [28]は、ユビキタスコンピューティングで利用するためのコンテキスト情報のモデリング手法として、5W1H に基づくモデリングとツール開発を行う研究である。この文献では、コンセプト・インスタンス・リレーションといったオントロジー工学の概念を、コンテ

キストに沿った概念にするために 5W1H を用いている。さまざまな概念を統一的にとらえるための枠組みという意味では、文献 [26]と関係がある。

文献 [29]は、医療情報へのアクセス制御に関するモデルの研究であり、6W1H を明確に記録した電子医療記録システム（Electronic Medical Record System, EMRS）を利用している。ここでは、who, when, where, why, whose, what, how が記録されている。誰が「誰の」医療記録を参照したのかを明示するために whose が用いられている。

文献 [30]は、ユビキタスな医療サービスのために、医療情報のプロトコル仕様として 6W1H を用いたモデルを利用する研究である。ここでは、医療情報のプロトコルとして 5W1H 以上に必要な点を考慮し、Where を Where-pre と Where-post の 2 つに分解している点が特徴である。

文献 [31]は、レガシーシステムを理解するためのリバース・リエンジニアリング手法として、5W1H を用いたモデリングを用いる研究である。この文献はソフトウェア中心のシステムを対象としているので、リエンジニアリングの結果は UML などのモデルを作成することを主眼としている。本論文の次章で紹介する防災業務のモデリングとは、レガシーシステムの理解のために 5W1H を用いてドキュメントを整理するという点で、共通する。

文献 [32]は、システム開発手法として近年注目されているアジャイル開発の一手法として「ユーザーストーリーマッピング」を提案する書籍である。これは、要件を「誰が、何を、なぜ」（すなわち、Who, What, Why）に着目して記述し、関係者で議論することで、ユーザにとって使いやすいサービス・商品を行うための手法である。

このように、5W1H、6W1H そのものは特定の研究分野を形成しない一方、これらを利用した研究や開発手法は多数存在する。表 4-1 に関連研究をまとめた。

文献	分野	5W1H への追加・改変	特色
[23]	システムエンジニアリング（プロジェクト管理）	How many, How much, Humanware	人間性の強調
[24]	システムエンジニアリング（ミッション解析）	Whom	ミッションの曖昧さをなくすことの強調
[25]	ビジネス分析	特になし	3W1H など、特定の項目を抜粋
[26]	ビッグデータ解析	特になし	アクションではなくデータの分類に利用
[27]	法科学（デジタルフォレンシクス解析）	Which	全体図を描くために利用
[28]	ユビキタスコンピューティング（オントロジー工学）	特になし	Context-aware なモデル構築が目的
[29]	医療情報システム	Whose	診療記録なので whose を利用
[30]	ユビキタスコンピューティング（医療サービス）	Where を Where-pre と Where-post に分解	タスクの開始場所と終了場所を明記
[31]	システムエンジニアリング（リバースエンジニアリング）	特になし	レガシーシステムの理解を目的
[32]	システムエンジニアリング（アジャイル開発）	特になし	Who, What, Why の 3 つのみ使用

表 4-1 5W1H 等を用いた手法・研究

4.2.2. システムエンジニアリングにおけるモデリングとの比較

システムエンジニアリングの分野では、ソフトウェアやサービスの開発を目的とした業務のモデリング技法が多数存在する。例えば、BPMN（ビジネスプロセスモデリング表記法）[33]や、UML [34]におけるアクティビティ図、ユースケース図などがある。

これは、システムの動的側面に着目したモデリング技法である。一方、6W1H モデルは、システムそのものより「システムの記述」を対象とした、システムの静的側面に着目したモデリング技法である。この差異は、BPMN 等がソフトウェアやサービスの開発を目的としている一方で、6W1H モデルはシステムアシュランス議論のオントロジー構築を目的としていることから生まれたものである。

6W1H モデルと、これらのモデリング技法は排他的ではない。すなわち、6W1H モデルが対象とするシステムを、BPMN や UML を用いてモデリングすることも可能である。

4.3. 6W1H モデルの構築法と考察

4.3.1. 構築法

関連研究を概観したところで、本論文が提案する 6W1H モデルの具体的な構築手順を示す。前提として、システムを記述した文書があるとする。

1. 文書から、記述すべきアクションの最上位の（すなわち、最も抽象度が高い）「What」を特定し、記す。
2. Who、Whom、When、Where、Why を、What の記述の近くや関係する項目を探して記す。見当たらなければ、システムのステークホルダと議論し、特定する。
   手順 1,2 で、ひとつのアクションが記述される。
3. 必要であれば、完成したアクションを複数のアクションに分割する。再び文書から「What」を特定し、記す。（以下繰り返し）

4.3.2. 「6W」の役割

6W1H モデルにおいて、1 つのアクションに付される 6 つのラベルは、複雑な文書からアクションを同定するために、以下の意味で有効であると考えられる。

1. 「What」は 6W の根本である。どのようなアクションであっても、What が明記されなければ実行できない。
2. 「Who」はアクションの主体を明らかにする。これは、日本語のような、主語が必須でない言語では特に効果的である。
3. 「Whom」によって、その Whom に記された人や組織が Who となる他のアクションがあることを示唆する。これはアクションの抜け漏れを防止する。
4. 「When」はアクションの順序を示唆する。この順序は、アクションの必要条件を議論する機会をステークホルダに提供する。
5. 「Where」はアクション間の伝達手段を明らかにする。アクションの結果が「情報」である場合は、それをどのように伝達するかが問題になる。防災業務のように、被災によって電話等の伝達手段が寸断される可能性のある場合、伝達手段を前もって明示することは特に重要である。
6. 「Why」はアクションの目的を強調する。アクションは、その「Why」で示される事柄を達成するために実行される。「Why」を明示することで、以下の事項が議論できる。

a. このアクションは親のアクションを実現するために必要か（他のアクションの子に移動すべきか）？

b. このアクションたちは、親のアクションを実現するのに十分か（さらにアクションを追加すべきか）？

4.3.3. 「1H」がなす階層の役割

6W1H モデルがなす木の階層（深さ）は、あるアクションの説明の詳細さに対応する。これは、システムに対する理解の程度が異なる様々なステークホルダが議論する際に有用である。例えば、あるソフトウェアをシステムとして考えるとき、システムのユーザにとっては、システムの機能の仕様が重要である。一方で、システムの開発者にとっては、その機能をどのように実装するかが重要であり、ある機能をより詳細に分解して議論する必要がある。このような、ステークホルダの種類に応じた説明を 6W1H モデルは提供する。

また、How による記述の木構造は、変更箇所の洗い出しを容易にする。あるレベルでアクションの記述を変更する際に、その子孫および親を辿ることで、変更すべき箇所の確認ができるからである。

4.4. 6W1H モデルによる「共通フレーム 2013」の分析

6W1H モデルは、既存文書に記されたアクションを構造化するために用いる。ここで、既存文書として、システムライフサイクルプロセス記述のガイダンスとして日本国内で標準的に利用されている「共通フレーム」の最新版「共通フレーム 2013」 [35]より、「合意契約の変更管理プロセス」を題材に、6W1H モデルの利用法を示す。

共通フレームは、システム開発のうち、特にソフトウェア開発のプロセスに重点を置いてプロセスを定めた文書である。システムの発注・受注およびその後の開発におけるやりとりをプロセスとして定めることで、関係者間の意思疎通を円滑にすることを目的としている。初版発行の 1994 年より何度か改訂され、ISO/IEC 12207 [36]として国際標準化されるなど、広く産業界で利用されている文書である。

合意契約の変更管理プロセスのうち、「協議の実施及び合意の形成」というアクティビティを題材にする。このアクティビティ 1.3.4 には 2 つのタスク 1.3.4.1, 1.3.4.2 がある。

1.3.4 協議の実施及び合意の形成
このアクティビティは、次のタスクからなる。
1.3.4.1 協議の実施
取得者および供給者は、協議の場において、当該契約変更要求の内容、要因、背景と当該変更を実施した場合のプロジェクト計画、費用、利益、品質及

び予定に与える影響を比較考慮し(b)、最適な結論を導くよう(a)協議を行う。

1.3.4.2 承認レベルのエスカレーションと合意の形成

特に費用負担の取り扱いにかかる協議に当たっては、必要に応じてエスカレーションを行い、経営層を含む適切な管理層による合意形成、決着を図る。

（ [35] P. 112　引用のため下線・ラベルを付加した）

タスク 1.3.4.1 を中心に検討する。この文章の主語は「取得者および供給者」であり、述語は「協議を行う」である。すなわち、一見すると 6W1H モデルの Who が「取得者および供給者」であり、What が「協議を行う」であると考えられる。

次に、下線部 a の記述を分析する。分析においては、目的と手段を注意深く考える必要がある。この文を見ると、「最適な結論を導く」ことが目的であると述べている。そして、「最適な結論を導く」ための手段が、さまざまな事項を比較考慮した協議であると考えるのが自然である。すなわち、1 つのタスクの記述のように見える部分は、実は粒度が異なる 2 つの記述が混在している。

また、下線部 a のうち、二重下線部 b も、大きく 2 つに分けられる。すなわち、「当該契約変更要求の内容、要因、背景」の比較考慮と、「当該変更を実施した場合のプロジェクト計画、費用、利益、品質及び予定に与える影響」の比較考慮である。前者は契約変更そのものに対する考慮であり、後者は契約変更した場合のプロジェクトに対する考慮である。

ここまでをまとめると、表 4-2 のようになる。

表 4-2 「協議の実施」タスクの 6W1H モデルによる検討

6W1H モデル	親タスク	子タスク 1	子タスク 2
Who	取得者および供給者	取得者および供給者	取得者および供給者
What	最適な結論を導く	当該契約変更要求の内容、要因、背景を比較考慮する	当該変更を実施した場合のプロジェクト計画、費用、利益、品質及び予定に与える影響を比較考慮する
Whom	?	?	?
When	?	?	?
Where	?	協議の場において	協議の場において
Why	?	最適な結論を導くため	最適な結論を導くため

現時点では確定できない項目には「?」を記した。親タスクとして「最適な結論を導く」があり、それを実現するために、Why が「最適な結論を導くため」であるふたつのタスクが存在するという構造が明らかになった。

元のタスクの記述は、実際のシステム開発現場に適用する際に解釈が必要である。解釈とは、抽象度の高い文言で記された語彙を、具体的な「その」システム開発の語彙に置き換えた上で、必要であれば記述を詳細化することである。例えば、上記のプロセスをあるシステム開発プロジェクトに適用する際、「取得者」や「供給者」は、実際のシステム発注者やシ

ステム受注業者に置き換えられる。「当該契約変更」は、実際に提案された契約変更によって置き換えることで、はじめて議論や検討の対象となる。さらに、「当該契約変更要求の内容」「当該契約変更要求の要因」「当該契約変更要求の背景」などを明らかにすることで、実際の比較考慮が可能になる。

6W1H モデルによる構造の明示は、その解釈を支援する。例えば、表 4-2 において、各タスクの Who には「取得者および供給者」と記されている一方、Whom は空欄である。実際には、契約変更要求は取得者か供給者のいずれかから提案されるものであると考えられる。また、協議にあたって、取得者から供給者に対しての説明があったり、供給者から取得者に対しての説明があったりするのが自然であろう。共通フレームでは、このような具体的なレベルのタスクまでは規定しない。6W1H モデルを利用することで、解釈する際の一方法として、Who と Whom をより細かくしたタスクを実施することが明らかになる。

表 4-2 で空欄の項目から、さらなる示唆を得ることができる。例えば、When は空欄である。すなわち、協議がいつどのような順序で実施されるかの記載がないことを示す。これは、具体的なシステム開発においてプロセスを適用する際には、どのタイミングで協議を実施するのかを決定する必要があることを示す。

また、タスク 1.3.4.2 の When は「必要に応じて」であると考えられる。すなわち、常に必要なタスクではないと示されていることが明らかになる。When には時間的な前後関係だけでなく、タスク発生の条件も記される。

ここまで、共通フレームの一アクティビティを事例にして、6W1H モデルによる分析で、具体的なタスクを明らかにできることを示した。共通フレームは前述のとおり、システム開発において広く用いられる文書であり、その内容理解と解釈が必要とされるものである。本節の適用例は、6W1H モデルの有効性を示すと考えられる。次章では引き続き、自治体防災業務が記された文書に対して 6W1H モデルを適用し、その有効性を検討する。

5. 事例研究：平塚市防災業務のオントロジー構築とアシュランス議論

本章では、前章で提案した 6W1H モデルを実際のアシュランス議論構築に適用した事例（発表リスト 1、発表リスト 2）を紹介する。アシュランス議論の進め方は以下の 3 つの段階に分けられる。

1. 防災業務を規定する既存の文書から、防災業務をシステムライフサイクルとして同定する。
2. オープンシステム・ディペンダビリティという性質を適切に定める。
3. 防災システムのライフサイクルがオープンシステム・ディペンダビリティを持つことを主張するアシュランスケースを構築する。

既存の文書から、防災業務をシステムライフサイクルとして同定することはひとつの課題である。防災業務を規定する文書である「地域防災計画」は、全体像をつかむことも、詳細を理解することも容易ではない文書である。

そこで、6W1H モデルによるモデリング技法を、平塚市地域防災計画に規定された給水業務のアシュランスケース構築によって例示した。給水業務の目的は、発災時に、被災者に対して水を供給することである。このモデリング技法によって、給水業務をシステムライフサイクルにおける「給水プロセス」として記述することができた。

5.1. 背景

5.1.1. 平塚市の防災業務

日本では、各自治体の防災業務は「地域防災計画」として文書化されている [37]。日本政府は「災害対策基本法」 [38]という法律を 1961 年に施行し、各都道府県や市町村が設置する「防災会議」、各都道府県防災会議や市町村防災会議が作成する「地域防災計画」を規定している。すなわち、日本国内には 1000 以上の地域防災計画が存在する。地域防災計画が対象とする災害は、自然災害（例：地震、津波、風水害、火山災害、雪害）と人為的災害（例：海上の油流出、原子力事故、鉄道、航空機事故）の両方である。各地域防災計画は、このような災害に対する、予防や準備、応急対策、復旧と復興に関する事項を記す。

著者の所属する大学が所在する神奈川県平塚市も、多くの災害リスクを抱えている。地震・台風は日本中で被害を受けうる。特に、相模湾に面する平塚市では、津波の危険もある。最新の津波浸水想定 [39]では、平塚市でも最大津波高さ 9.6m の津波が予測されている。さらに、平塚市から 30km ほどしか離れていない箱根では、近年火山活動が活発である。

このような災害リスクに対して、平塚市地域防災計画は 1960 年代より何度も改訂を重ねた結果、非常に膨大で複雑な文書となった。表 5-1 は平塚市地域防災計画の構成である。資

料編を含めると総ページ数は 700 ページを超える。本研究では、地震発生時の応急対策 [40] に焦点を当てる。

表 5-1 平塚市地域防災計画（平成 27 年 3 月改訂）の構成

冊子名	ページ数
地震災害対策計画	196
風水害対策計画	181
東海地震に係る地震防災強化計画	24
特殊災害対策計画	33
資料編	288

5.1.2. オープンシステム・ディペンダビリティ（OSD）

ディペンダビリティは、日本語では「信頼性」もしくは「総合信頼性」と訳される用語で、国際標準 IEC 60050-192 [41]では" ability to perform as and when required"（要求された時に要求されたように振る舞う能力）と定義されている。

オープンシステム・ディペンダビリティ [11]（以下 OSD）とは、システムをオープンなもの、すなわちシステムの境界や機能・構造は時間とともに変化し、異なる視点から絶えず異なって認識される、と見做した上でシステムが持つべきディペンダビリティのことである。D-Case（アシュランスケースの拡張）や D-Case in Agda （形式アシュランスケース記述ツール） [15] [16]など、OSD 達成を示すためのさまざまな手法が提案されている。国際標準 IEC 62853 Open Systems Dependability [7]が発行予定である。この標準では OSD を以下のように定義している。

> ability to accommodate changes in purpose, objectives, environment and actual performance and to achieve accountability continually, so as to provide expected services as and when required （要求されたときに要求されたように期待されたサービスを提供するために、目的、目標、環境や実際の振る舞いの変化に対応し、絶えず説明責任を遂行する能力）([7] 3.13)

自治体の防災業務も「オープンシステム」と見做すことができ、OSD 達成を問う対象である。なぜなら、防災業務は災害のリスク評価（例：地震の被害想定）や、国内外の規制（例：原子力発電所からの放射線許容量）、世論などによって変化するからである。

5.2. システム記述における課題：発災時の給水業務

本節では、地域防災計画理解に際しての２つの課題を説明する。それは、（１）システムの全体像を把握すること（２）システムを詳細に理解すること、である。

一般に、システムアシュランス議論を実施する前提として、ステークホルダがシステムを理解する必要がある。理解のためには、全体像を大まかに把握するというトップダウンの視点と、詳細な業務を理解して、それらがどのように全体のなかで位置付けられるかを把握するというボトムアップの視点が必要である。

本節では例として、災害発生時の給水業務をとる。給水業務とは、発災時に被災者へ水を供給する業務である。この業務には、水の確保、供給のための準備、給水車の移動、避難所での水の供給やその他の関連する活動が含まれる。なお、日常的な上下水道の提供は含まない。

5.2.1. システムの全体像を把握する

システムの全体像を把握することの困難さの事例として、2 つの表どうしの対応関係が不明な例を挙げる。表 5-2 と表 5-3 はいずれも、平塚市地域防災計画に記された地震発生時の給水業務の一覧である。

表 5-2 平塚市災害対策本部分担業務（出典： [45] p.13,抜粋）

給水部	◎市民部長	給水班	◎協働推進課長 ○市民課長 ○人権・男女共同参画課長	1　飲料水の確保に関すること。 2　避難所等への給水及び搬送に関すること。 3　水道営業所等関係機関との連絡調整に関すること。 4　他団体等からの応援給水に関すること。 5　応急対策特命に関すること。

平塚市役所の防災担当者によると、表 5-2 は発災時の各部署のすべての業務を定めた表の一部である。一方、表 5-3 は給水業務のみを定めた節に記載されている。よって、表 5-3 は表 5-2 を詳細化したものであるべきである。表 5-2 の 1 つの業務が、表 5-3 で複数の個別の業務に分割されているのが適切である。

しかし、そのような望ましい対応はこの２つの表にはない。例えば、表 5-2 の１「飲料水等の確保に関すること」は、表 5-3 の①②④に対応するように見える。また、表 5-2 の２「避難所等への給水及び搬送に関すること」は、表 5-3 の②③④⑤に対応するように見える。しかも、この対応関係はこの地域防災計画に記載されていないし、市の担当者であれば自明というわけでもない。

表 5-3 給水業務の分担（出典： [40] p.131）

関係部等	分担業務
給水部	① 被害状況、復旧の見通し等給水に関する情報収集及び県企業庁平塚水道営業所、協定締結事業者との連絡、調整 ② 飲料水等の全般的な必要給水量の把握、給水場所及び給水方法等の調整 ③ 給水用タンクの確保及び総務部を通じてトラック協会等運送関係機関への協力要請 ④ 飲料水等の確保並びに給水場所及び医療機関への搬送、給水 ⑤ 非常用貯水タンクによる給水 ⑥ 応援協定都市、県、自衛隊等の協力に関する総合対策部への要請、受入れ及び業務の調整

5.2.2. システムを詳細に理解する

システムを詳細に理解することの困難さを示す事例として、業務記述に不備がある例を示す。表 5-4 は給水業務における水の確保の詳細を示す記述の抜粋である。

表 5-4 飲料水等の確保の順序及び方法（出典： [40] p.133）

確保の順序	確保の方法
第１次確保	① 広報、自主防災組織等を通じ、市民、事業所等に対し、飲料水の「汲み置き」を呼び掛け、確保します。 ② 道路状況に特に支障のない場合は、神奈川県企業庁の災害用指定配水池（平塚配水池）から、給水車又は給水容器を用いて搬送し、飲料水又は医療用水を確保します。 ③ 協定に基づき、協定締結事業者から飲料水を確保します。

②の記述「道路状況に特に支障のない場合は、神奈川県企業庁の災害用指定配水池（平塚配水池）から、給水車又は給水容器を用いて搬送し、飲料水又は医療用水を確保します。」に着目する。一見すると、曖昧な表現はなく、１つの作業を適切に表現しているように見える。しかし、以下の不備がある。

- 「道路状況に特に支障のない場合は」は、道路の被害状況を給水業務担当者が特に問題なく知ることができることを仮定している。しかし、誰が被害状況を調査するのか、その調査結果をどのように知ることができるかは不明である。

- この文には主語がない。誰が水を確保し、誰が水を搬送するのかは不明である。

5.2.3. 課題の考察

以上で見たように、現在の地域防災計画の記述は、直接的に防災「システム」の記述であると見做すことは難しい。内容を解釈し、ISO/IEC/IEEE 15288 を適用してシステムライフサイクルプロセスを構築することも容易ではない。また、著者らが他の市町村の地域防災計画を調査したところ、このような地域防災計画の複雑さは、平塚市地域防災計画に限った問題ではないことも明らかになった。

災害対策基本法 [38]では、防災業務として「何を記述すべきか」は定めているが、「どのように記述すべきか」までは規定していない。規定する箇所は以下である。

> 第四十二条　2　市町村地域防災計画は、おおむね次に掲げる事項について定めるものとする。
>
> 一　当該市町村の地域に係る防災に関し、当該市町村及び当該市町村の区域内の公共的団体その他防災上重要な施設の管理者（第四項において「当該市町村等」という。）の処理すべき事務又は業務の大綱
>
> 二　当該市町村の地域に係る防災施設の新設又は改良、防災のための調査研究、教育及び訓練その他の災害予防、情報の収集及び伝達、災害に関する予報又は警報の発令及び伝達、避難、消火、水防、救難、救助、衛生その他の災害応急対策並びに災害復旧に関する事項別の計画
>
> 三　当該市町村の地域に係る災害に関する前号に掲げる措置に要する労務、施設、設備、物資、資金等の整備、備蓄、調達、配分、輸送、通信等に関する計画

「どのように記述すべきか」を規定しない結果、各自治体の地域防災計画の記述様式は統一されず、その記述の複雑さが増大する要因となったと考えられる。6W1H によるモデリングは、システムに関する複雑な記述を、システムライフサイクルプロセスのオントロジーとして整理するための手法である。

5.3. 6W1H モデルを用いた「給水システムオントロジー」の構築

本節では、前節の事例に 6W1H によるモデリング手法を適用し、アシュランス議論を構

築する。地域防災計画に記された給水業務から、給水システムの 6W1H 記述を作成する[8]。そして、その記述をもとにアシュランスケースを作成する。

5.3.1. 全体像が把握できるオントロジーの構築

給水システムの記述を、高さ 2 の木として構成した（図 5-1)。これは表 5-2、表 5-3 や文献 [40]にある関係する文、そして市の防災担当職員との議論をもとにした。

まず、アクション W（市民の生命・身体の保護のため、災害対策本部は発災時に避難所で被災者に水を供給する）を記述した。これは、ISO/IEC/IEEE 15288 のプロセス・アクティビティ・タスクの三層構造のうち「プロセス」に相当する記述である。これは、平塚市地域防災計画地震編 [40]で発災時の給水業務を記した部分の冒頭にある以下の文章を元にした。

> 被災者に対する飲料水、生活用水及び医療用水（以下、本節においては「飲料水等」という。）の供給は市長が行います。ただし、災害救助法が適用された際は県知事が行うが、県知事から委託を受けた場合には市長が行います。（ [40] 4.9.1(1)実施機関）

なお、ここ「供給は市長が行う」と記されていることの意味は、供給業務実施の「責任」が市長にあることであり、実際の業務は各担当者が行うものであると市の防災担当職員から説明があった。また、「市民の生命・身体の保護のため」という Why の部分は、計画の冒頭にある以下の記述から導いた。

> この計画は、災害対策基本法（昭和 36 年法律第 223 号。以下「災対法」という。）第 42 条の規定に基づき、本市域に係る地震災害対策に関し、減災に向けたまちづくり、平常時の対策、災害時の応急対策、災害復旧・復興対策等について必要な事項を定め、本市防災関係組織の総力を結集して防災活動を総合的かつ計画的に実施することにより、市民の生命、身体、財産を災害から保護するとともに、災害による被害を最小限に止め、もって社会秩序の維持と公共の福祉の確保に資することを目的とします。（ [40]1.1.1(1)計画の目的）

次に、アクション W を三つの基本的なアクション W1、W2、W3 に分割した。すなわち、給水実施／終了の判断、給水業務の準備、給水業務の実施である（いずれも What に示される)。これらは、ISO/IEC/IEEE 15288 におけるプロセス・アクティビティ・タスクのうち「ア

[8] 作成する「給水システムの 6W1H モデル」は、「給水システムライフサイクルプロセス」と言える。このようなプロセスは ISO/IEC/IEEE 15288 に存在しないプロセスであるが、この標準では新しいプロセスを作成することが許されている（2.1.4 節で述べたシステムライフサイクルプロセスのテーラリング)。

クティビティ」に相当する記述である。アクションを 3 分割した理由は、現状の表 5-2 と表 5-3 の記述を系統的にまとめる枠組みを市の防災担当職員と検討し、何かの業務を実施する際には「情報を収集し、その業務を実施するかどうか、実施中の場合は終了するかどうかを判断する」「実施するとなった場合、実施に向けて準備する」「実際に実施する」という 3 つに分けるのが自然であるという結論に達したためである。この分類は、一般に言われる PDCA（Plan, Do, Check, Act）を CA, P, D の 3 つに分けたことに相当する。

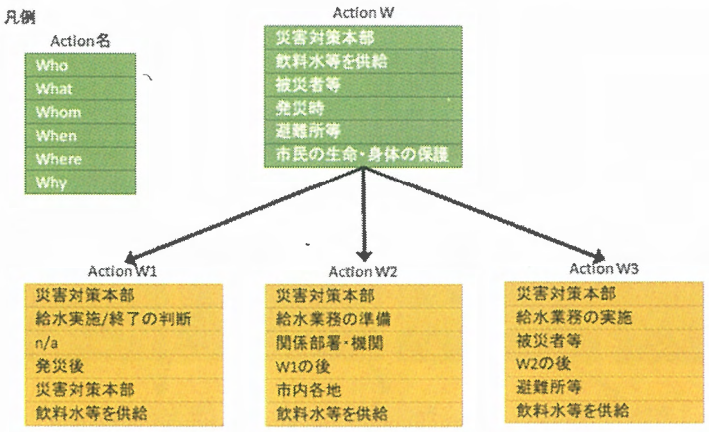

図 5-1　6W1H モデルによる給水プロセスの記述（上部）

5.3.2. 詳細が理解できるオントロジーの構築

図 5-1 の 6W1H モデルを詳細化し、表 5-4②の一文から 7 つのアクションを作成した（図 5-2）。アクション W、W1、W2、W3 は図 5-1 と同一である。これらは、ISO/IEC/IEEE 15288 におけるプロセス・アクティビティ・タスクのうち「タスク」に相当する記述である。

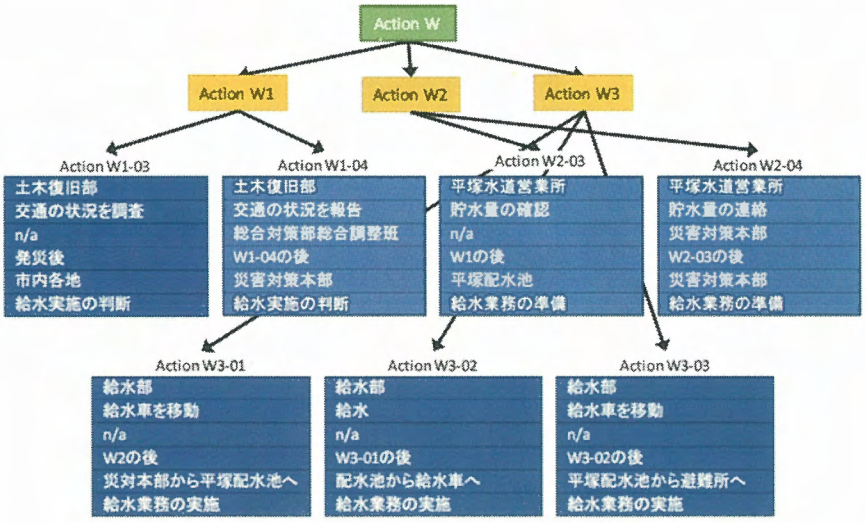

図 5-2　6W1H による給水プロセス記述の詳細化（抜粋）

以下に、表 5-4②の一文と、各アクションの対応を示す。

「道路状況に特に支障のない場合は」

- W1-03「交通の状況を調査」
- W1-04「交通の状況を報告」

「神奈川県企業庁の災害用指定配水池（平塚配水池）から」「飲料水又は医療用水を確保します」

- W2-03「貯水量の確認」
- W2-04「貯水量の連絡」

「給水車又は給水容器を用いて搬送し」

- W3-01「配水池への給水車の移動」
- W3-02「配水池から給水車への給水」
- W3-03「給水車を避難所へ移動」

いくつかの記述は、文献 [40]の別の部分にあった記述や、市の防災担当職員との議論によって追加された。以下はその例である。

- 「土木復旧部」（W1-03、W1-04 の What）は文献 [40]の別の部分にあった。
- 「平塚水道営業所」（W2-03、W2-04 の What）は、議論によって明らかになった。
- 搬送業務は準備ではなく実施段階での業務であることが、議論によって明らかに

なった。

- 「飲料水」と「医療用水」は同じ水を指すことが、議論によって明らかになった。

これらは、6W1H によるモデリングの枠組みが、システムを詳細に理解するための明確なシステムの記述を促進することを示す。結果として、W1 の子として 7 つのアクションが、W2 の子として 23 個のアクションが、W3 の子として 19 個のアクションが記述された。付録 A に 6W1H モデルの全体を記す。

5.3.3. 関連研究：防災業務のモデリング

本節では、6W1H モデルを用いて、自治体防災業務のシステムとしてモデリングした。自治体の防災業務をシステムとしてモデリングする研究は、著者が知る限り少ないながら存在する。Sommerville らの文献 [42]は responsibility modelling [43]をイギリスの洪水対策プランの解析に用いている。彼らの目的は複雑な文書を解析し、理解を深めることであり、我々の目的とも通ずる。彼らが開発したモデルは「responsibility（責任）」に重点をおいており、それはステークホルダの関係によって表現される。

この責任の関係は、6W1H モデルにおいては、How がなす親子関係によって表現される。例えば、図 5-1 と図 5-2 のアクション W1 と W1-03 は文献 [43]の意味で以下の事項を表す。

- 土木復旧部は交通の状況調査に責任を持つ
- 災害対策本部は、その責任の所有者（authority）である。

5.4. 6W1H モデルに基づくアシュランスケースの構築

本節の内容は、（発表リスト 2）に基づく。

5.4.1. システムが機能要件を満たすことを主張するアシュランスケースの構築

6W1H の階層的な木構造から、以下の手順でアシュランスケースを構築することができる。

1. 6W1H モデルの各アクションの 6W から、ゴールおよびサブゴールを記述する。
2. 各ゴールとサブゴールを、適切なストラテジーによって接続する。
3. サブゴールに対して、エビデンスを与える。
4. 6W1H モデルで用いた語彙をコンテキストとしてまとめる。

各サブゴールのエビデンスの一例として、アクションの実施結果報告が考えられる。平塚市の防災業務では、防災訓練の結果報告書がそれにあたる。

この手順に従って作成したアシュランスケースが図 5-3 である。この 6W1H モデルからは、議論のパターンを見出すことができる。すなわち、図 5-1 で示した基本的なアクション (Action W1, W2, W3) である「供給の決定」「供給の準備」「給水の実施」は、「決定、準備、実施」という議論パターンを示唆する。この議論パターンは、発災時の応急対応業務においては、食料供給や人的支援などにも適用可能であると考えられる。

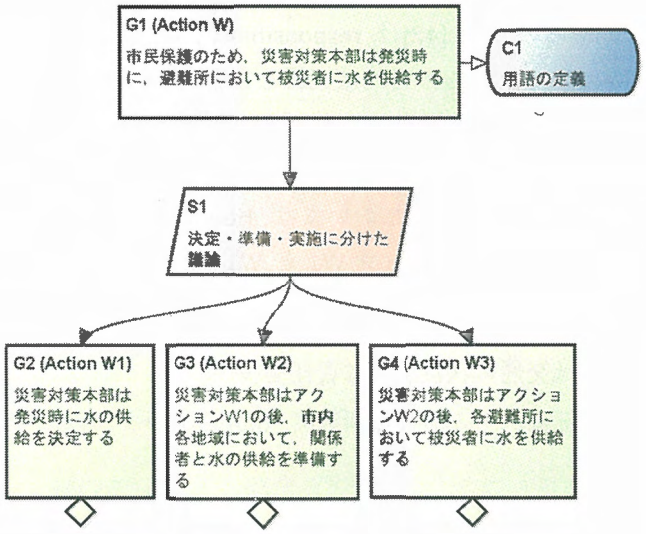

図 5-3 「決定・準備・実施」の議論パターン

5.4.2. システムが OSD を満たすことを主張するアシュランスケースの構築

IEC 62853 [7]に記載されているアシュランスケースのテンプレートが図 5-4 である（日本語訳は著者による)。前節で構築した図 5-3 のアシュランスケースは黄色のゴール G6「対象システム固有の要件が達成される」の一部である。平塚市の防災システムが OSD 要件を達成することを示すためには、G6 以外のサブゴール G2, G3, G4, G5 が達成されることを示す必要がある。これは、以下の手順で行った。

1. オープンシステム・ディペンダビリティの要件を定める国際標準案 IEC 62853 が示す要件および、アシュランスケースのテンプレートを理解する
2. その要件は一般のシステムに対して示されているので、それを平塚市の防災業務に即して解釈する
3. 解釈した要件と現在の平塚市地域防災計画の記述とを比較し、要件が満たされているかどうかを判断する。満たされているならば、アシュランスケースにエビデンスとして付加する。

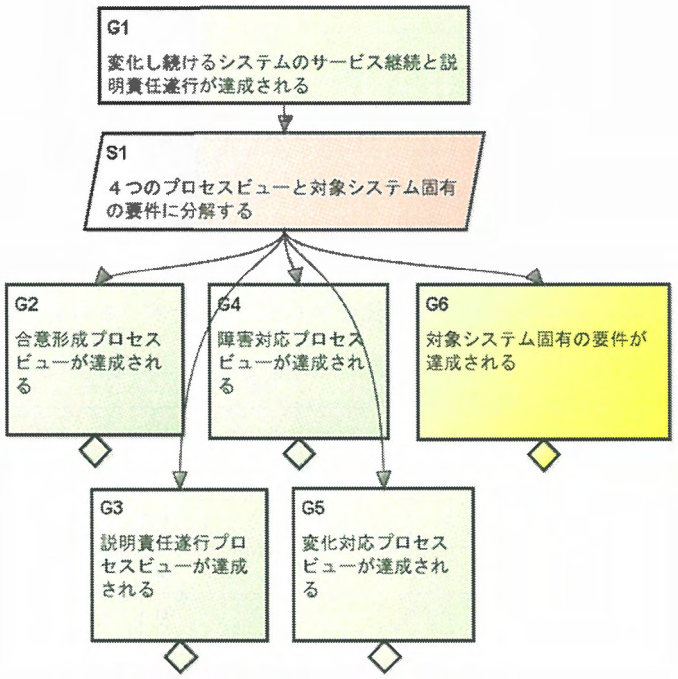

図 5-4 OSD 達成を主張するアシュランスケースの全体構造

一般的なアシュランスケース構築においては、3 は、ゴールをより詳細なサブゴールに分割し、それぞれが満たされているかどうかの議論を実施する。しかし、本研究では各ゴールが満たされているかどうか、3 段階で評価した。ここで、3 段階とは以下である。

A) ゴールを示す明確な証拠がある

B) ゴールを示す証拠がいくつかあるが、そうとは明記されていない。また、それらはゴール達成に必要であるが、十分であるとは言えない

C) ゴールを示す証拠がない

このように評価を実施した理由は、アシュランスの達成度を、大まかではあるが短期間で判定するためである。すなわち、「ゴールを示す証拠がない」ことが明らかであれば、IEC 62853 が示す OSD 要件を詳細化する必要がなくなる。

上記 1 から 3 の手順に従って OSD 達成を検討した結果、対応度は表 5-5 のようになった。対応する記述が十分である項目（対応度 A）は 3 つであった一方、対応する記述がない項目（対応度 C）が 29 個であった。

対応する記述がない項目が多数発見されたことは、IEC 62853 が、地域防災計画として記述すべき事項への指針を与えていることを示す。一般に、地域防災計画においては、大きな災害が発生した後に、そこで得た教訓を反映させる改訂を実施してきた。例えば、1995 年に発生した阪神淡路大震災の後に、復興計画に関する記述が大幅に追加されたことや、2011 年に発生した東日本大震災の後に、津波の被害想定見直しや、津波からの避難計画が拡充されたことなどが挙げられる。本研究におけるアシュランスケース構築は、システムエンジニ

アリング、特に OSD の観点から、防災業務として現在不足している事項を明らかにする効果があると考えられる。

検討結果の詳細を、付録 B にしるす。

表 5-5 平塚市の防災業務が OSD を満たすことの対応度

対応度	A	B	C
合計	3	30	29
合意形成	1	6	5
説明責任遂行	1	8	4
変化対応	0	7	15
障害対応	1	9	5

5.5. 明確なオントロジーを持つ業務記述の作成指針

前節では、6W1H モデルによって業務をシステムライフサイクルプロセスとして記述し、それを元にアシュランス議論をアシュランスケースとして構築する方法を述べた。本節では、さらに一歩進んで、「明確なオントロジーを持つ業務記述の様式」とはどのようなものかの指針を示す。本章の事例では「明確なオントロジーを持つ平塚市地域防災計画の様式とは、どのようなものか」ということに相当する。

本章の事例研究においては、平塚市地域防災計画の複雑な記述を整理し、関係者によるアシュランス議論を促進するために、6W1H モデルを利用した。しかし、「平塚市地域防災計画」そのものと、「平塚市地域防災計画の 6W1H モデルによる表記」は別の文書である。この 2 つを継続的に維持管理することは困難であるし、望ましくない。望ましい姿は、平塚市地域防災計画における業務の記述が、6W1H モデルと自明に変換可能な様式で記述されていることである。

また、自明に変換可能であるだけでは十分とは言えない。なぜなら、平塚市地域防災計画は、業務だけを記述する文書ではないからである。例えば業務とは、ある状態を別の状態に更新する作業であると考えられるから、業務を明確に記述するためには、その前後の「状態」も明らかにすべきであろう。これは「業務のオントロジー」とも言える。本節では、このような事項を検討し、地域防災計画、さらには一般の業務記述として望ましい様式を明らかにする。

概要

明確なオントロジーを持つ業務記述のためには、以下の 8 つの点に留意して記述すべきであると考える。

1. 用語の定義と参照を区別する
2. 文の参照と非参照を区別する
3. 文のうち「業務を定める文」と、「状況を定める文」を区別する
4. 「業務を定める文」では、「主要業務」と「支援業務」を区別する
5. 「状況を定める文」では、「現状」「将来の状況（問題あり）」「将来の状況（問題なし）」を区別する
6. 「業務を定める文」に、必要項目（6W1H）が明記されている
7. 「状況を定める文」に、必要項目が明記されている
8. 文書全体の整合性が定期的に見直される

これらの関係を図 5-5 に示す。以下の各節では、平塚市地域防災計画より具体的な例を挙げつつ詳説する。

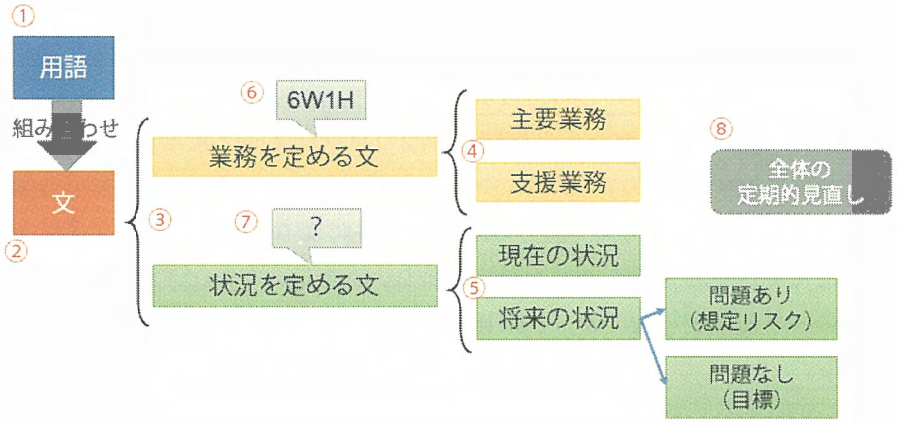

図 5-5　明確なオントロジーを持つ業務記述に必要な 8 項目

5.5.1. 用語の定義と参照を区別する

まず、文を構成する小さな単位である用語の検討を行う。業務を記述するためには文が必要である。文は、固有の業務を記述するための用語を使って記述される。用語の解釈が関係者によって異なると、議論は困難である。

用語の解釈の違いを関係者間で減らすためには、以下の 2 点に注意する必要がある。

1. 用語の定義を文書中に記載する。
2. 定義された用語のみを使用（参照）して、文を記述する。

現在の記述

> 被災者に対する飲料水、生活用水及び医療用水（以下、本節においては「飲料水等」という。）の供給は市長が行います。（ [40] 4.9.1(1)）

この文は、発災時の給水業務に関する節の最初の一文である。この文は、供給する水の種類には「飲料水」「生活用水」「医療用水」の 3 つがあり、それらを総称して「飲料水等」とすることを示している。

問題点

飲料水・生活用水・医療用水とはどのようなものかという定義は、この部分のみならず、地域防災計画に記載がない。定義がないまま、以下のように本文で用語が利用（参照）されている。

> 医療用水の供給は、水道、井戸等の施設が破壊され、医療用水が汚染し、又は断水したため、現に医療用水を得ることができない医療機関に対して行います。（ [40] 4.9.1(3)ア）

市の防災担当者によると、医療用水とは何なのかを関係機関に問い合わせた結果、特別に医療用に特殊な水を手配しておくというわけではないことが判明したそうである。

修正の指針

用語を定義し、定義した用語を使って文を記述すべきである。このことは、業務を明確に記述するための必要条件である。用語の定義がない場合、関係者が文を正確に理解することが困難になる。

5.5.2. 文の参照と非参照を区別する

用語に続いて、文が持つべき性質を検討する。文では、「参照」と「非参照」という考え方を利用すると、文書の構造を整理することができる。

これは、用語の「定義」と「参照」から得た着想である。用語の「定義」と「参照」は、「非参照」と「参照」の関係である。例えば、定義が変更になった場合、それを参照して利用している箇所は、そのままの記述でよいか確認する必要がある。このような関係が文同士にもある。

5.2.1 節で紹介した 2 つの表の説明をもう一度見る。

- 表 5-2 は発災時の各部署のすべての業務を定めた表の一部である。
- 表 5-3 は給水業務のみを定めた節に記載されている。
- よって、表 5-3 は表 5-2 を詳細化したものであるべきである。
- 表 5-2 の 1 つの業務が、表 5-3 で複数の個別の業務に分割されているのが適切である。

これは、表 5-2 の各文が「非参照」であり、表 5-3 の各文が「参照」であることを示している。用語の定義・参照とは異なり、参照にあたる文の中に、直接的に非参照側の文は現れない。6W1H モデルにおける「How」による詳細化も、このような「参照」と「非参照」の一例であると考えられる。

現在の記述

5.2.1 節で紹介した 2 つの表

- 表 5-2 資料編 p.13 平塚市災害対策本部分担業務 のうち給水部の記述
- 表 5-3 地震編 p.131 給水業務の分担

問題点

同じ給水業務を定めているにも関わらず、参照と非参照の関係が明らかでない。

修正の指針

参照と非参照の関係を検討し、明記する。検討の結果、そのような関係がないのであれば、文を修正・削除する。

5.5.3. 文のうち「業務を定める文」と、「状況を定める文」を区別する

続いて、文を２つに分類する。２つとは、「業務を定める文」と「状況を定める文」である。

業務とは、ある状況（状態）を別の状況に変化させるものであると考えられる。そのため、業務を明確に記述するためには、どのような状況を、どのような状況に変化させるものであるのかを、明らかにすることが望ましい。また、ひとつの文において、業務の記述と状況の記述が混在すると、文の理解が困難になる。これらは、区別して記述することが望ましい。

現在の記述

> 市では、南関東地震被害想定の避難者数に基づき、209,860 人を目標に、長期保存食の備蓄を進めています。([40] 3.8 <現状>)

この記述は、物資供給に関する対策の現状を箇条書きで示したもののひとつである。この記述がある第３章では、各節で「現状」「課題」「今後の取り組みの方向」という３点に着目し、箇条書きがなされている。この３つの名前から察するに、上記の文が記された「現状」には状況を定める文が入るのが自然である。

問題点

上記の文には物資供給の状況だけではなく、物資供給の業務も記述されている。この文には３つの要素がある。

- 市は長期保存食の備蓄を進めている（平常時の業務）
- 209,860 人の長期保存食の備蓄がある（将来目指す状況）
- 南関東地震被害想定の避難者数（将来目指す状況の根拠）

実は、現在何人分の備蓄があるのかという「現状」の記述がない。これは、「市は長期保存食の備蓄を進めている」という業務を、状況と混同していることから生じている問題である。

この混同が生じる一因は、業務も「業務を進めているという状況」という広い意味では「状況」であると考えられるためである。状況とは、ある視点から客観的に世界を眺めたものであるから、俯瞰的な視点に立てば、すべての業務は状況であるとも言える。一方、業務とは、業務を行う主体が存在し、その主体の視点から主観的に述べられるものである。

修正の指針

視点を業務主体（市や、具体的な担当部署）に固定し、業務と状況を区別して記述する。それにより、文の理解が容易になると考えられる。

5.5.4. 「業務を定める文」では、「主要業務」と「支援業務」を区別する

前節であげた文の 2 類型のうち 1 つ、「業務を定める文」が持つべき性質を検討する。業務を定める文は、業務の種類によって 2 つに分類すべきである。2 つとは、「主要業務」と「支援業務」である。

主要業務とは、目的達成のためにそれが必須である業務である。いくつか存在することもあるが、1 つでも欠けると、防災業務としての目的が達成されないものである。

対して、支援業務とは、主要業務の円滑な推進のために、補助的に行われる業務のことである。これは、仮に欠けていたとしても、主要業務自体は推進される。しかし、支援業務があった方が、主要業務は円滑に進めることができる。

図 5-6 平塚市地域防災計画に記された 9 業務

平塚市地域防災計画を分析し、さまざまな業務を主要業務と支援業務を分類したのが図 5-6 である。主要業務として、物資供給・避難支援・医療・救急・インフラ復旧・建物復旧・衛星の 7 業務がある。それらの支援業務として、応援受け入れ・管理の 2 業務があると考えた。

現在の記述

発災時の対策を述べた文献 [40]の第 4 章「災害時の応急対策」の見出しは以下の表 5-6 である。

問題点

似た業務が別の箇所に記載されている。例えば、第 16 節「広域的応援体制」では、応援受け入れ業務を定める。一方、第 9 節にも「1(7) 他の自治体等への応援要請及び受入れ」という項目がある。

修正の指針

ひとつの節にはひとつの業務だけを記述する。この方針で記述することで、実際に主に担当する部署、関係する部署が、自身に関係する箇所を網羅的にチェックする必要がなくなる。

表 5-6 平塚市地域防災計画地震編第 4 章の見出し

項目	見出し
第 1 節	災害対策本部の設置と運営
第 2 節	公共施設の応急対応
第 3 節	災害時情報の収集と伝達
第 4 節	救急・救助、消火及び医療救護活動
第 5 節	避難対策
第 6 節	津波対策
第 7 節	災害廃棄物等の処理対策
第 8 節	保健衛生、防疫、遺体の処理等に関する活動
第 9 節	飲料水、食料及び生活必需物資等の調達・供給活動
第 10 節	教育対策
第 11 節	緊急輸送のための交通の確保、緊急輸送活動
第 12 節	県警察・第三管区海上保安本部の取組み
第 13 節	ライフラインの応急復旧活動
第 14 節	自主防災組織等の活動
第 15 節	災害ボランティアの活動
第 16 節	広域的応援体制
第 17 節	災害救助法関係
第 18 節	二次災害の防止活動

5.5.5. 「状況を定める文」では、「現状」「将来の状況（問題あり）」「将来の状況（問題なし）」を区別する

本節では文の 2 類型の 2 つ目「状況を定める文」が持つべき性質を検討する。これは、まず時系列で「現状（現在の状況）」と「将来の状況」に二分する。続いて、将来の状況は「問題あり」と「問題なし」に二分する。

まず、「現状」と「将来の状況」の二分について検討する。これは一般に言われる「過去、現在、未来」という 3 区分ではなく、「これまで」と「これから」という 2 区分に基づく考え方であるものの、本質的な相違はない。「過去、現在、未来」という 3 区分は、過去と未来に時間の幅がある一方、現在だけが点として存在している。

「問題あり」と「問題なし」の 2 区分は、時系列に対応して、業務記述が 2 つに分類できると考えて作成した。

1. 「現状（の問題）」を業務によって解決し、「将来の状況（問題なし）」をつくる
2. 「将来の状況（問題あり）」を業務によって解決し、「将来の状況（問題なし）」をつくる

以下にそれぞれの例を示す。

例 1 :「現状（の問題）」→業務→「将来の状況（問題なし）」

現在の記述

> 市では、南関東地震被害想定の避難者数に基づき、209,860 人を目標に、長期保存食の備蓄を進めています。([40] 3.8 <現状>)

問題点

「現状」という節の記述であるにも関わらず、現状の記載がない。

修正の指針

以下の枠組みを用いて分析し、抜けている記述を補足する。

- 現状： （？人分の備蓄がある）
- 業務： 長期保存食の備蓄
- 将来の状況（問題なし）： 209,860 人分の備蓄がある

例２：「将来の状況（問題あり）」→業務→「将来の状況（問題なし）」

将来の状況（問題あり）とは、一般にリスクと呼ばれるものである。例えば、以下の文はリスクを指摘している。

現在の記述

> 相模川や金目川流域の一部地域では津波の河川遡上による浸水の可能性があり、早急な堤防整備が必要です。([40] 2.4 <課題>)

問題点

堤防整備した結果、どのような状況を作り出せばよいのか明らかでない。

修正の指針

以下の枠組みを用いて分析し、抜けている記述を補足する。

- 将来の状況（問題あり）：　津波の河川遡上による浸水
- 業務：　堤防整備
- 将来の状況（問題なし）：　（津波が河川遡上せず、浸水しない）

また、この分析により、「何ｍの津波を対象とするのか？」「相模川や金目川流域の一部地域とはどこなのか？」「堤防を整備するだけで十分なのか？」といった事項の気づきも得やすくなると考えられる。

5.5.6. 「業務を定める文」に、必要項目（6W1H）が明記されている

ここまで、文の 2 類型「業務を定める文」「状況を定める文」それぞれに対して、さらに詳細な区分を検討した。本節と次節では、文にどのような項目を記述すべきかを、類型ごとに検討する。本節では、「業務を定める文」が持つべき項目を検討する。

「業務を定める文」が持つべき項目は、本論文で提案した「6W1H モデル」に準じることを提案する。すなわち、6W（Who, What, Whom, Where, When, Why）を一文にもれなく記し、さらなる詳細化が必要であれば、それを複数の 6W によって分解する（How）。

現在の記述

> 火災の発生がない場合は、消防部と協議し、各避難所において消火栓に臨時給水栓を取り付け、飲料水を確保します。([40] 4.9.1(5)飲料水の確保)

問題点

誰がこの業務を行うか明らかでない。

修正の指針

以下のように 6W1H モデルの 6W を用いて整理する。

- Who ： （記載なし）
- What ： 消火栓に臨時給水栓を取り付ける
- Whom ： （人に対して行う業務ではないので、なし）
- Where ： 各避難所において
- When ： 火災の発生がない場合
- Why： 飲料水を確保するため

この枠組みを用いることで、Who の記載がないことが明らかになる。また、除外した「消防部と協議」の部分に関しても「何を協議するのか？」「どのような協議結果となれば、臨時給水栓を取り付けるのか？」といった事項への気づきを得ることができる。

6W1H モデルという枠組みを用いることで、ただ文章を読むだけでは見落としがちな、存在しない記載の発見が可能になる。

5.5.7. 「状況を定める文」に、必要項目が明記されている

本節では、「状況を定める文」が持つべき項目を検討する。持つべき項目に関しては、一定の結論は出ておらず、今後の研究が必要である。しかし、業務を定める文と同様、使用されている用語の意味を明らかにすることは必須である。

一例を示し、今後の方向性を示す。

> 大規模災害に備えて、被災者が一時的に避難するために小中学校等を避難所（55 か所）として指定しています。([40] 3.5<現状>)

この文は以下のような状況を定めている。

- 状況： 55 か所の小中学校は、避難所に指定されている
- その目的： 大規模災害時に被災者が一時的に避難すること

少なくとも、状況を記述するためには、「何の状況か」という主体（ここでは「小中学校」）が必要である。そして、その主体の状況（ここでは「避難所に指定されている」）も述べられる必要がある。さらに、「避難所に指定されている」とはどういうことなのか、という用語の定義があることが望ましいと思われる。

さらなる例を考察し、必要な枠組みを帰納的に検討することは今後の課題である。

5.5.8. 文書全体の整合性が定期的に見直される

ここまで、用語および文が持つべき性質を考察した。本節では最後に、用語および文によって構成される文書全体が持つべき性質を検討する。重要なのは、「文書全体の整合性が定期的に見直されること」である。

一般に、業務を記述した文書は、現実の業務を反映すべきものである。しかし、文書自体は自動的に現実を反映して更新されるわけではない。そのため、現実の状況に即した記述がなされているかを定期的に確認し、即していない場合は修正する必要がある。

現在の記述

地域防災計画自身の見直しに関する以下の記述がある。

> この計画は、本市を取り巻く社会情勢の変化や防災環境の変化等を踏まえ、常に実情に沿った計画とするため、災対法第 42 条の規定に基づき、毎年上記にある実施状況の点検等を行い、必要があると認めるときは県、関係機関等と協議、調整を行った上で修正をします。([40] 1.5.2)

問題点

この記述は、前述した「現実と文書との整合性維持」のために必要であるが、十分であるとはいえない。すなわち、「実施状況の点検等」に何が含まれるのかが明らかではない。どの項目を、どのように点検するのかを明らかにすることが望ましい。

修正の指針

点検の具体化には、5.5 節でこれまで述べた業務記述の方式が大いに貢献すると考えられる。すわなち、6W1H モデルや、「業務」と「状況」といった区分を使うことによって、「この現状は本当に現状と一致しているか」「この業務の目的はこう書かれているが、それは本当に必要なことか」といった判定項目の発見を容易にすることができると考えられる。

以上、5.5 節では 8 項目にわたって、明確なオントロジーを持つ業務記述様式に関する指針を示した。この 8 項目は少なくとも必要であると考えられる一方、これで十分であるかの検討は、今後の課題である。

6. おわりに

6.1. 結論

本論文では、システムアシュランス議論をより効果的に行うための、システムのオントロジー構築法を示した。特に、システムライフサイクルプロセスをオントロジーとして記述するための枠組みとして「6W1H モデル」を提案し、その有効性を自治体防災業務という事例研究で確かめた。

得られた結論は以下である。対応する節を括弧内に示した。

- 6W1H モデルによって、平塚市地域防災計画における発災時の給水業務の記述を「給水システムライフサイクルプロセス」として構造化できた。主語などの抜け漏れが発見できることを定量的に示した。市の防災担当職員からは、モデリングが有効であるとの定性的評価を得た。(5.3)
- 6W1H モデルから、システムが機能要件を満たすことを主張するアシュランスケースが、一定の手順で構築できることを示した。(5.4.1)
- アシュランスケース構築において、ゴールへの対応度を 3 段階にて評価する手法を考案した。平塚市の防災業務が OSD を満たすことを主張するアシュランスケース構築に適用し、信頼性の観点から地域防災計画に不足している記述を見つけ出した (5.4.2)
- 「共通フレーム 2013」への適用を事例として、6W1H モデルは防災業務の分析に限らず、プロセス記述の分析に利用できることを示した。(4.4)
- 明確なオントロジーを持つ業務記述の作成指針を提案し、平塚市地域防災計画によって例示した。(5.5)

6.2. 今後の課題

社会技術システムへの適用実験

本論文で提案した 6W1H モデルは、システムライフサイクルプロセスの一部として定める人間の作業をモデル化するものである。そこで、そのような人間の作業も含めた社会のシステム (社会技術システム、 Socio Technical System) をモデル化し、そのアシュランス議論を行うことは有効ではないかと推測する。例えば、食料品の安全、政策決定の妥当性などである。

この方向の正当性は、アシュランスケースの拡大の歴史から推察できる。まず、アシュランスケースは、安全性を問うセーフティケースから始まり、性質を安全性だけでなく、その他の性質にも一般化することでアシュランスケースとなった。これは、アシュランスケース

がパラメータとして持つ２つの要素「システム」「システムの性質」のうち、後者「システムの性質」の一般化である。

当然、「システムの性質」だけでなく、対象となる「システム」も一般化できる。アシュランスケースは、従来は高信頼性が求められるソフトウェア・ハードウェア中心のシステムに対して構築されることが多かった。これは、アシュランスケース構築・維持に時間や要員のコストがかかることが一因である。形式アシュランスケースのような、アシュランスケースの構築や維持管理を容易にする概念・手法が普及すれば、本論文でも事例研究として挙げた自治体防災業務のようなシステムに広く適用可能であると考えられる。

6W1H モデルにおける階層の基準策定

6W1H モデルは、6 つの W でアクションを記述したのち、それを複数のアクションに分割・詳細化し、木を構成する。木の階層構造は、さまざまなステークホルダが関与するシステムアシュランス議論において、あるアクションを説明する粒度を、ステークホルダの理解度に応じて提供する。ただし、どのような粒度で木を構築するのが適切か、という点は本研究の対象としなかった。

この粒度には、システムごと、あるいはシステムに関与するステークホルダの分類ごとに、一定の基準があるのではないかと考えられる。例えば一般的なシステム開発であれば、要件定義、基本設計、詳細設計、実装といった区分（階層）があり、それらは関与するステークホルダ（ビジネス層、設計者、開発者等）ごとに分類されていると考えられる。

システムアシュランス議論を円滑に進めるためのテンプレートとして、このような基準あるいは基準作成の指針の研究が必要である。

6W1H モデルとして適切な数理的モデル

本論文で提案した 6W1H モデルは、木構造を持つと定めた。しかし、モデリングとして木以外の構造が適切である可能性は議論しなかった。木以外の構造として、例えばグラフ、その中でも木に似た構造を持つ有向非巡回グラフ（Directed acyclic graph, DAG）が考えられる。6W1H モデルとして適切な数理的モデルの検討が必要である。

システムが持つべき性質のオントロジー構築法

3.1 節で述べたように、「議論に適したオントロジーをどのように構築するか」という課題には２つの観点があった。すなわち、

1. 「システム」のオントロジーをどのように構築するか
2. 「（システムが持つべき）性質」のオントロジーをどのように構築するか

である。6W1H モデルは、前者のオントロジー構築法を提案するものであり、後者は本論文では対象としなかった。より厳密なシステムアシュランス議論の方法論確立のためには、この研究が必要である。

安全性、セキュリティ、ユーザビリティ、事例研究でも述べたオープンシステム・ディペ

ンダビリティなど、持つべき性質は様々に考えうる。それらを厳密に議論するためには、安全であるとはどういうことか、セキュアであるとはどういうことか、といったことを検討し、より詳細な定義を構築する必要がある。そのときに利用できる共通の枠組みが求められる。

システムにおいては、例えばその枠組みは「システムライフサイクルプロセス」という概念であったり、その記述法「6W1H モデル」であったりした。システムの性質に対しても、同様な枠組みを考案することが今後の課題である。

形式アシュランスケース構築ツールの実用化

第 2 章で紹介した形式アシュランスケースと、プログラミング言語 Agda によるその実装は、膨大かつ複雑になるシステムアシュランス議論を支える技術要素である。しかし、これらはシステムアシュランス議論の現場でまだ普及していない。普及のためには、さらなる理論研究と実証実験の両方が必要である。

理論面では、形式アシュランスケースの数理的モデルをより精密にする必要がある。2.2.4 節では形式理論とその証明がアシュランスケースとどう対応するかを示した。しかし、複雑なアシュランスケースの記法の完全な形式化（パラメータを持つアシュランスケース等の文法を、BNF 記法等で表現すること）は、アシュランスケースの国際標準 ISO/IEC 15026-2 [9]でも未だなされていない。これを明らかにすることで、アシュランスケース構築の計算機による支援がより促進される。

実証面では、プログラミング言語 Agda のような自動での整合性検査可能な構造を内部的には持ちつつ、プログラミングに不慣れなシステムのステークホルダであっても容易に利用できるインタフェースをもつツールが必要である。そのようなツールの試作と実証実験を今後進める必要がある。

また、本研究で提案した 6W1H モデルに関しても、形式アシュランスケースの一部として位置づけるための、更なる研究が必要である。例えば、Agda による形式アシュランスケースとしての記述実験が考えられる。

さらに 6W1H モデル自体の構築および維持管理にかかる負担を削減することが、実用化に必要である。既存文書を分析し、半自動的に 6W1H モデルを構築するツールの研究開発が必要である。

付録 A　給水プロセスの 6W1H モデルによる表現

第 5 章で紹介した、平塚市地域防災計画を元に作成した、発災時における給水プロセスの 6W1H モデルによる表現を以下に記す。紙面の都合で、木構造ではなく、表形式で記載する。「ID」列の W はプロセス、W1, W2, W3 はアクティビティ、W1-01, 02 などは、各アクティビティの子にあたるタスクを示す。

なお、Who の列が赤字になっているものは、平塚市地域防災計画では主語が明記されていなかったタスクを示す。これは、49 個のうち 19 個にのぼった。

ID	Who	What	Whom	When	Where	Why
W	災害対策本部	飲料水等を供給	被災者等	発災時	避難所等	市民の生命・身体の保護
W1	災害対策本部	給水の実施/終了を判断	×	発災後	災害対策本部設置場所	飲料水等を供給
W1-01	総務部被害調査班、特別調査班	水道の被害状況を調査	×	発災後	市内各地	給水の実施/終了を判断
W1-02	総務部被害調査班、特別調査班	水道の被害状況を報告	総合対策部総合調整班	W1-01 の後	×	給水の実施/終了を判断
W1-03	土木復旧部	交通の状況を調査	×	発災後	市内各地	給水の実施/終了を判断
W1-04	土木復旧部	交通の状況を報告	総合対策部総合調整班	W1-03 の後	×	給水の実施/終了を判断
W1-05	給水部	給水体制の進行状況等を調査	×	給水開始後	×	給水の実施/終了を判断
W1-06	給水部	給水体制の進行状況等を報告	総合対策部総合調整班	W1-05 の後	×	給水の実施/終了を判断
W1-07	災害対策本部	給水の実施を判断	×	W1-02,04,06 の後	災害対策本部設置場所	給水の実施/終了を判断
W2	災害対策本部	給水業務を準備	被災者等	W1 の後	市内各地	飲料水等を供給
W2-01	総合対策部広報班	汲み置きを連絡	自主防災組織	W1 の後	×	飲料水の確保
W2-02	自主防災組織	汲み置きを呼びかけ	被災者等	W2-01 の後	×	飲料水の確保
W2-03	県企業庁平塚水道営業所	貯水量を確認	×	W1 の後	平塚配水池	供給可能量の把握
W2-04	県企業庁平塚水道営業所	貯水量を連絡	災害対策本部	W2-03 の後	×	供給可能量の把握
W2-05	協定締結事業者	飲料水の状況を確認	×	W1 の後	事業所	供給可能量の把握
W2-06	協定締結事業者	飲料水の状況を連絡	災害対策本部	W2-05 の後	×	供給可能量の把握
W2-07	給水部	非常用貯水タンクの状況を確認	×	W1 の後	非常用貯水タンク所在地	供給可能量の把握
W2-08	給水部	非常用貯水タンクの状況を連絡	災害対策本部	W2-07 の後	×	供給可能量の把握
W2-09	消防部	火災の状況を確認	×	W1 の後	災害対策本部	供給可能量の把握
W2-10	給水部	臨時給水栓の設置を協議	消防部	W2-09 の後	×	供給可能量の把握
W2-11	医療機関等	給水量の把握	×	W1 の後	医療機関等	需要量の把握

ID	Who	What	Whom	When	Where	Why
W2-12	医療機関等	給水の要請	給水部	W2-11 の後	×	需要量の把握
W2-13	避難部	給水量の把握	×	W1 の後	避難所	需要量の把握
W2-14	避難部	給水の要請	給水部	W2-13 の後	×	需要量の把握
W2-15	住宅・公園部	給水量の把握	×	W1 の後	公園等	需要量の把握
W2-16	住宅・公園部	給水の要請	給水部	W2-15 の後	×	需要量の把握
W2-17	給水部	備蓄資機材を調達	×	W1 の後	資機材備蓄場所	給水業務準備
W2-18	給水部	運搬車両の調達を要請	総務部総務班	W1 の後	×	給水業務準備
W2-19	総務部総務班	運搬車両を調達	トラック協会等	W2-18 の後	×	給水業務準備
W2-20	給水部	自家発電機燃料の調達を要請	総務部総務班	W2-07 の後	×	給水業務準備
W2-21	総務部総務班	自家発電機燃料を調達	×	W2-20 の後	×	給水業務準備
W2-22	給水部	搬送の方法を決定	×	W1 の後	災害対策本部設置場所	給水業務準備
W2-23	給水部	搬送の地域割りを決定	×	W1 の後	災害対策本部設置場所	給水業務準備
W3	災害対策本部	給水業務を実施	被災者等	W2 の後	避難所等	飲料水等を供給
W3-01	給水部	給水車を移動	×	W2 の後	元の場所から平塚配水池へ	給水業務の実施
W3-02	給水部	飲料水を移送	×	W3-01 の後	平塚配水池から給水車へ	給水業務の実施
W3-03	給水部	給水車を移動	×	W3-02 の後	平塚配水池から目的地へ	給水業務の実施
W3-04	給水部	給水車を移動	×	W2 の後	元の場所から各事業所へ	給水業務の実施
W3-05	給水部	飲料水を移送	×	W3-04 の後	事業所	給水業務の実施
W3-06	給水部	給水車を移動	×	W3-05 の後	事業所から目的地へ	給水業務の実施
W3-07	給水部	給水車を移動	×	W2 の後	元の場所から非常用貯水タンク所在地へ	給水業務の実施
W3-08	給水部	飲料水を移送	×	W3-07 の後	非常用貯水タンク所在地	給水業務の実施
W3-09	給水部	給水車を移動	×	W3-08 の後	非常用貯水タンク所在地から目的地へ	給水業務の実施
W3-10	市民、事業所	水道水を汲み置き	×	W2 の後	自宅、各事業所	飲料水の確保

ID	Who	What	Whom	When	Where	Why
W3-11	避難所運営委員会等	飲料水を供給	被災者等	W3-03,06,09 の後	目的地	給水業務の実施
W3-12	給水部、避難部	臨時給水栓を設置	×	W2 の後	消火栓所在地	給水業務の実施
W3-13	避難所運営委員会等	飲料水を供給	被災者等	W3-12 の後	消火栓所在地	給水業務の実施
W3-14	避難部	ろ水機を移動	×	W2 の後	保管場所から利用場所へ	給水業務の実施
W3-15	避難部	耐震性プールの水をろ過	×	W3-14 の後	ろ水機利用場所	給水業務の実施
W3-16	避難所運営委員会等	耐震性プールの水を供給	被災者等	W3-15 の後	ろ水機利用場所	給水業務の実施
W3-17	県企業庁平塚水道営業所	配水管を復旧	×	W2 の後	配水管故障個所	給水業務の実施
W3-18	県企業庁平塚水道営業所	応急給水栓を設置	×	W3-17 の後	避難所等	給水業務の実施
W3-19	県企業庁平塚水道営業所	飲料水を供給	被災者等	W3-18 の後	応急給水栓所在地	給水業務の実施

付録 B　　平塚市の防災業務が OSD 要件を満たすことの検討

5.4.2 節にて紹介した、平塚市の防災業務がオープンシステム・ディペンダビリティ（OSD）を持つことの検討結果が次ページの表である。ここでは、市の防災システムのうち、特に発災時の供給システムを中心に検討した。表は以下の手順に従って作成した。

1. IEC 62853 (Open Systems Dependability) [7]の第 6 章に記載されている、OSD 要件 62 個を日本語訳する。
   - この要件は Outcome（達成されたときのシステムの状態）として記されている。ISO/IEC/IEEE 15288 の Outcome と同じ意味である。
   - この翻訳は、平塚市担当者と内容に関して議論するために必要であったものである。
2. 翻訳した要件を、平塚市の発災時供給システムにおいて解釈する。
   - この結果「Outcome の平塚市発災時供給システムでの解釈」列が完成する。
3. 解釈した各要件に対して、それを満たす証拠を平塚市地域防災計画から探す。
   - 証拠を発見すれば、「対応証拠の記述箇所」にその箇所を、「対応する理由」列に対応すると思われる理由を記す。
   - 証拠を発見しなければ、空欄とする。
   - いずれの場合でも、「現状ないが必要な証拠の記述」列に、要件を満たすために必要であるが、現在欠けている記述を記載する。（証拠が発見された場合でも、それだけで十分とは限らない。必要な証拠が他にもあるかもしれない）
4. 以上の結果を元に、対応度を A、B、C の 3 段階で記載する。それぞれの意味は以下のとおりである。
   - A 対応する記述があり、明示されている。この記述で十分であると考えられる。
   - B 対応する記述はあるが、そうとは明示されていない。また、その記述だけでは十分とは言えない。
   - C 対応する記述はない。

この手順に従って表を作成した結果を次ページ以降に記す。以下は本文 表 5-5 の再掲である。対応する記述が十分である項目（対応度 A）は 3 つであった一方、対応する記述がない項目（対応度 C）が 29 個であった。このことは、IEC 62853 が、地域防災計画として記述すべき事項への指針を与えていることを示す。

対応度	A	B	C
合計	3	30	29
合意形成	1	6	5
説明責任遂行	1	8	4
変化対応	0	7	15
障害対応	1	9	5

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.2.2	合意形成プロセスビュー				
6.2.2 a)	a) 供給システムのステークホルダ間でシステム等に関する共通理解と明示的合意が確立している。「システム等」とはシステム、システムの目的、目標、環境、性能、ライフサイクルおよびそれらの変化を言う。				
6.2.2 a)1)	a)1)平塚市発災時供給システムのステークホルダが同定されている。	A	地震編 1-6 地震編 4-9 担当部・担当機関	1-6 には防災業務全般の担当が、4-9 にはそのうち供給システムに関係する担当が明記されている。	（特になし）
6.2.2 a)2)	a)2)記述の枠組（供給システムで用いる用語の定義や、供給システムの基本的な前提）が確立しており、すべてのステークホルダによって理解されている。	C			供給システム（供給活動・供給業務）とは何を指すか、給水とは何かなど、基本的な用語を定義した用語集があることが望ましい。また、供給業務の前提（3 日間は動けない可能性もある）といった前提事項も明らかにすることが望ましい。
6.2.2 a)3)	a)3) 供給システム等（目的、目標、環境、実施、ライフサイクルとそれらの変化）についての各ステークホルダによる共通理解が得られている。共通理解には、システムの前提と、ステークホルダの責任についての理解を含む。	B	地震編 4-9 のうち、供給システムを定める記述	供給システムが何を行うかについては、現状の記述で一定の共通理解が得られると考えられる。また、ステークホルダの責任についての記述（市長など）もある。	目的、目標、環境、実施、ライフサイクル等がわかりやすい記述にすることが望ましい。特に、業務そのものの記述と、条件によって業務を変更する記述（ライフサイクル）とが、いずれも人間のアクションであるため、区別が難しい。これを分けた記述が望ましい。
6.2.2 a)4)	a)4) 供給システムに関して合意に達しない場合の調停のプロセスが定められている。	C			地域防災計画（の供給システムの記述）がどのような手順・体制で作成・合意されるかの策定プロセスの記述があることが望ましい。これは、必ずしも地域防災計画内に記述する必要はないと考えられる。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.2.2 a)5)	a)5) 供給システムの目標、目的等の理解に基づいて、供給システムに関する明示的合意が得られ、記録されている。 記録には、合意形成過程の説明と、合意事項が適切かつ実現可能であると見なされた理由を含む。	B	平塚市防災会議の会議録	会議録は、明示的合意を記録する文書であると考えられる。	「合意形成過程の説明と、合意事項が適切かつ実現可能であると見なされた理由」が記載されることが望ましい。現状、変更箇所について承認されていることは読み取れるが、全体について合意しているかは明らかではない。 防災会議レベル（地域防災計画全体）では困難だとしても、供給システム等、各個別業務のステークホルダ間で合意したことを記録することが望ましい。
6.2.2 a)6)	a)6) 供給システムに関する合意文書の解釈のステークホルダによる差異は十分に小さい。	B	平塚市防災会議の会議録	会議録は、明示的合意を記録する文書であると考えられる。	上記と同様で、「合意文書の解釈のステークホルダによる差異は十分に小さい」ことが示されることが望ましい。これも、各個別業務のステークホルダ間で合意したことを記録することが望ましい。
6.2.2 a)7)	a)7) 以上のアウトカムが公正に、供給システムの全てのステークホルダに配慮された方法で達成されている。	B	パブリックコメント実施の記録（Web サイト等）	パブリックコメントにより、システムからサービスを受ける側のステークホルダ「市民」に配慮している。	パブリックコメントの実施とその結果の公開だけなく、地域防災計画自体の決定過程を市の Web サイト等で公開することが望ましい。それにより、公正さの確認が容易になる。
6.2.2 b)	b) 供給システムのステークホルダ間で、システム等に関する共通理解と明示的合意が維持されている。				
6.2.2 b)1)	b)1)供給システムについての共通理解と明示的な合意を管理するポリシーが確立している。	B	1-5(P.16)	「今後の取り組み」の点検、環境の変化の把握、それらを踏まえた修正の記述は、システムについての共通理解（に必要な防災計画）の管理のポリシーにあたる。	地域防災計画に関する明示的な合意を管理するポリシーがあることが望ましい。すなわち、どのように地域防災計画が修正、合意されるかのプロセスの記述と、そのプロセスをどのような場合に見直し、修正するかの方針、である。
6.2.2 b)2)	b)2) 供給システムの目標、ステークホルダのニーズ、システム、環境などが変化しても明示的合意が維持されている。	B	平塚市防災会議の会議録	会議録は、明示的合意が維持されていることを記録する文書であると考えられる。	各個別業務のステークホルダ間で合意したことを記録することが望ましい。
6.2.2 b)3)	b)3) 供給システムの事業目標、ステークホルダのニーズ、システム、環境などが変化した時には、合意達成のプロセスが見直される。	C			まず、合意達成のプロセスの記述があることが望ましい。次に、それらがシステムの周辺の変化によって変更されることを明記することが望ましい。（例：地域防災計画の修正の種類によって、パブリックコメント実施の有無が決まる）

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.2.2 b)4)	b)4) 供給システムのアシュランスケースの構築と承認に関する責任が定められている。	C			必ずしもアシュランスケースの記法を採用する必要はないが、供給システム（の記述）がなぜそのようになっているかを記録した文書があることが望ましい。
6.2.2 b)5)	b)5) 供給システムにおける合意内容、合意形成過程の説明、合意事項が適切かつ実現可能であると見なされた理由がアシュランスケースに記録されている。	C			供給システムが一定の条件下で確かに動作するよう準備されていることを示すアシュランスケースがあることが望ましい。それには、供給システムが何をするかという合意内容、合意形成過程の説明、合意事項が適切かつ実現可能であると見なされた理由を記載すべきである。
6.3.2	説明責任遂行プロセスビュー				
6.3.2 a)	a) 供給システムのライフサイクルを制御する主要意思決定事項とリスクが同定されている。主要意思決定事項の中には、プロセスやプロセスビューのアウトカムを制御するものも含む。	B	4-9-1(4)ア(ア)	給水実施を総合的に判断するという記述は、主要意思決定事項にあたる。	1）誰が決定するのかを記述することが望ましい 2）給水だけでなく、物資や食料についても決定事項の記述があることが望ましい。 3）供給システムのライフサイクルにおけるリスクの記述があることが望ましい。
6.3.2 b)	b) 供給システムのライフサイクルを制御する各主要意思決定事項について、その責任者あるいは責任組織が同定されている。	A	4-9 担当部, 4-9-1(1)(2), 4-9-2(1)(2), 4-9-3(1)(2)	実施機関が市長であるということは、最終的な責任者は市長であることを示す。また、担当部は、責任組織を示す。	--
6.3.2 c)	c) 各合意の破綻（失敗や不履行）について、それを導く主要意思決定事項が同定されている。	C			供給システムのレベルで、合意事項と、主要意思決定事項との対応表があることが望ましい。
6.3.2 d)	d) 各合意の破綻が、責任を負わないステークホルダや一般社会に及ぼす影響が、分析され評価されている。	B	3-8	直接の分析と評価ではないが、そのようなものがあった結果、備蓄を呼び掛けていると考えられる	各合意について、その破綻がおよぼす影響が分析され、評価されることが望ましい。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.3.2 e)	e) 各合意の破綻がもたらす結末が合意されている。結末とは、責任者がどのような形で責任を取るのか、被害を受けたステークホルダや一般社会がどのような補償を得るのかなどである。	C			責任や補償についての記述があることが望ましい。ただし、応急対応は必ずしもうまくいくものではなく、補償の必要はない、という前提に被災者も合意しているとすれば、補償の記述は必要がない。
6.3.2 f)	f) 各主要意思決定事項について、その成果がモニターされ、評価されている。 これには合意事項の不履行のモニターも含む。	C			発災時に何を供給したかの記録およびその評価を行う仕組みを作り、それについて防災計画に記述することが望ましい。
6.3.2 g)	g) 意思決定を行うものと他のステークホルダに意思決定の結果を知らせるフィードバックループが確立している。	B	4-3-2, 4-3-3	4-3-2 では発災時の広報活動について定め、4-3-3 では発災時の情報収集について定めている。	資料編 2-1 や地震編 4-3-3 では、情報が収集されることは示されているが、意思決定の結果がどのように各部班に示されるかが明確ではなく、これを明記することが望ましい。
6.3.2 h)	h) 合意事項の不履行があった場合、責任者は遅滞なく是正活動を開始し、しかるべき補償を他のステークホルダ及び一般社会にもたらす。	C			合意事項の不履行（発災時に起こった問題）に遅滞なく対応する体制の記述があることが望ましい。
6.3.2 i)	i) 十分かつ適切な情報が責任者から他のステークホルダに対して遅滞なく提供される。				
6.3.2 i)1)	i)1) 供給システムに関する情報を渡すよう、合法的要求がステークホルダから寄せられれば、迅速かつ正確で十分な回答が与えられる。	B	4-3-1, 4-3-2(1)エ, 4-3-3(2)	4-3-3(2)では、迅速な対応のために窓口が設置されることが記述されている。また、それを支えるために通信設備について 4-3-1 に、情報収集について 4-3-2 に記載がある。	本ゴールの達成を議論し、アシュランスケースとして記録することで、関係者間での議論が促進されると考えられる。また、供給システムのように各個別システムレベルでの準備がなされていることが示されることが望ましい。
6.3.2 i)2)	i)2) 供給システムに関して提供された情報に対して、ステークホルダは正当な確信を持っている。	B	4-3	4 章 3 節全体として、正確な情報が収集・管理されるよう努めていることが示されている。	本ゴールの達成を議論し、アシュランスケースとして記録することで、関係者間での議論が促進されると考えられる。また、供給システムのように各個別システムレベルでの準備がなされていることが示されることが望ましい。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.3.2 i)3)	i)3) 障害時には、十分で適切な情報が選ばれて、供給システムのステークホルダのみならず、連結した他のシステムのステークホルダや公衆に対して提供される。	B	4-3	4章3節全体として、正確な情報が収集・管理されるよう努めていることが示されている。	本ゴールの達成を議論し、アシュランスケースとして記録することで、関係者間での議論が促進されると考えられる。また、供給システムのように各個別システムレベルでの準備がなされていることが示されることが望ましい。
6.3.2 i)4)	i)4) 供給システムへの要求、期待、記述、性能などの変化に関する情報の中から適切なものが選ばれて、供給システムのステークホルダ、連結した他のシステムのステークホルダや公衆に対して提供される。	B	3-8	3章8節の記述は、供給システムへの要求等の変化に関する情報であり、それが関係者に提供されることを示している。	本ゴールの達成を議論し、アシュランスケースとして記録することで、関係者間での議論が促進されると考えられる。
6.3.2 i)5)	i)5) 供給システムの要求、期待、記述、性能の間の差異の情報が見つかった場合には、適切なものが選ばれて供給システムのステークホルダ、連結した他のシステムのステークホルダや公衆に対して提供される。	B	3-8	3章8節の記述は、供給システムへの要求等に差異があった場合に修正されるものであると考えられる。	本ゴールの達成を議論し、アシュランスケースとして記録することで、関係者間での議論が促進されると考えられる。
6.4.2	障害対応プロセスビュー				
6.4.2 a)	a) 障害対応が準備されている。				
6.4.2 a)1)	a)1) 障害発生時に保護されるべき供給システムの主要機能が同定されている。	B	4-9-1(2)の表、4-9-2(2)イの表、4-9-3(2)イの表	主要な機能のみをまとめて記載しているので、これを中心に保護すべきであるとみなせる。	「主要機能は...である」「問題が発生した場合でも、この業務は優先して継続すべきである」といった記載があることが望ましい。 これは、BCPマニュアルに記載されている「発災時でも継続すべき通常業務」の考えにも通じるものである。 また、資料編1－5別表第2との整合性を図ることが望ましい。
6.4.2 a)2)	a)2) 供給システムによる物資提供を継続するために必要な主要機能保護活動のゴールが同定されている。	B	4-9-1(7)、4-9-2(6)、4-9-3(7)	例えば給水においては「給水量が不足する場合又は人員、資機材等の確保が困難であるときは」とあり、（1）需要にあった給水を行うこと（2）そのために必要な人員と資機材を確保することが、保護活動のゴールであるとみなせる。	システムの主要機能　と、主要機能保護活動　とが一見して区別できることが望ましい。現状、どちらも人間のアクションであるため、区別することが難しい。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.4.2 a)3)	a)3) 1)で定めた供給システムの主要機能に影響を与える故障、エラー、障害及びこれらの前兆が同定されている。	B	4-9-1(7)、4-9-2(6)、4-9-3(7)	例えば給水においては「給水量が不足する場合又は人員、資機材等の確保が困難であるときは」とあり、（1）給水量の不足（2）人員、資機材等の確保が困難は、障害とみなせる。	各主要機能に対して、それらの故障や障害が表などで対応づけられ、整理されていることが望ましい。例えば、地域防災計画では、上記を実施する旨を記し、各部班のマニュアルで具体的に整理する、といった手順が考えられる。
6.4.2 a)4)	a)4) 供給システムの同定された故障等の重要度解析及び影響分析が遂行されている。	C			どの物資が不足するのが一番問題か(重要度解析）、不足するとどのようなことが起きるか（影響分析）等を実施し、その結果を記録することが望ましい。
6.4.2 a)5)	a)5) 供給システム継続のために必要な、同定された故障等の処理のゴールが定義され、合意されている。	C			上記 a)3)でリストアップされた故障や障害それぞれについて、そのゴール（どうなればよいか、どの程度対応すればよいか）が整理されることが望ましい。
6.4.2 a)6)	a)6) 供給システムの各故障等の処理が、以下のいずれに属するかが同定されている。 i) 故障等の有無が監視され、故障等が起きた場合の処理が設計に組み込まれる。 ii) 故障等の有無が監視されるが、故障等が起きた場合の処理は設計に組み込まれない。 iii) 故障等の有無が監視されず、故障等が起きた場合の処理も設計に組み込まれない。	C			左に記した i) ii) iii)の分類に従って、各業務の障害とその対応が整理されることが望ましい。
6.4.2 a)7)	a)7) 6）i)の故障等に対しては、供給システムの主要機能保護のために、その故障等に対して指定された処理が開発されている。また 6)ii)及び 6)iii)に対しては、供給システムの主要機能保護のためのデフォルト処理が組み込まれている。	B	4-9-1(5)	第 1 次確保（主要機能）で道路状況に支障がある場合は、第 2 次～第 5 次確保（主要機能の故障に対して指定された処理）を行うと考えられる。（ただし、第 2 次～第 5 次確保も主要機能であると考えることもできる）	a)6)i)ii)iii)の定義にしたがって、指定された処理が記載されていることが望ましい。
6.4.2 a)8)	a)8) 供給システムに起きた原因不明の障害に対して、被害を減らすための一般的な方策が開発されている。	B	4-9-1(7)	原因が不明であっても、水や要員等が不足する場合は他の自治体に応援を要請するという記述は、「減災のための一般的な方策」にあたる。	a)3)で同定された障害それぞれに対して、一般的な方策が用意されているかどうかを明らかにすることが望ましい。
6.4.2 b)	b) 障害発生時に障害対応が遂行される。				

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.4.2 b)1)	b)1) 供給システムに故障等が発生した場合には検知される。	B	4-3-2(4)	道路状況について土木復旧部が調査するという記述があり、問題が検知できることを示している。	a)3)で同定された障害それぞれに対して、問題が検知できることが示されていることが望ましい。（これは地域防災計画に必ずしも記載されている必要はなく、別に報告書等の書類があればよい）
6.4.2 b)2)	b)2) 供給システムに実際に起こった故障等の原因分析、重要度解析及び影響分析が遂行されている。	C			a)4)と同様に、どの物資が不足するのが一番問題か(重要度解析）、不足するとどのようなことが起きるか（影響分析）等を実際に起きた障害に対して実施し、その結果を記録することが望ましい。
6.4.2 b)3)	b)3) 検知された障害等の処理のゴールが、状況に応じて更新されている。	C			a)5)と同様に、上記 a)3)でリストアップされた故障や障害それぞれの対応のゴール（どうなればよいか、どの程度対応すればよいか）が、実際に起きた障害対応の結果によって更新されることが望ましい。
6.4.2 b)4)	b)4) 供給システムに起こった故障等が 6）i)に属する場合には主要機能保護のためにその故障等に対して指定された処理が、6)ii)及び 6)iii)に属する場合には主要機能保護のためのデフォルト処理が、それぞれ遂行されている。	C			a)7)と同様に、a)6)i)ii)iii)の定義にしたがって指定された処理が遂行されることが望ましい。
6.4.2 b)5)	b)5) 供給システムに起こった故障等が 6)ii)及び 6)iii)に属する場合には、デフォルト処理以外の処理が、必要に応じてなされている。	C			a)6)ii)iii)の設計に組み込まれない処理については、事前に準備したデフォルト処理だけでなく、その場で臨機応変に対応を考え、実行することが望ましい。
6.4.2 b)6)	b)6) 供給システムに対して行う故障等の処理が、被害を拡大したり、他の危険を被るリスクを増加させたりしない。	C			b)4)と 5)で行われた処理が被害を拡大したり、他の危険を被るリスクを増加させたりしないことを示すことが望ましい。
6.4.2 b)7)	b)7) 供給システムへの被害だけでなく、連結された外部のシステムへの被害も含めて、全体として被害が減少している。	C			部分的な被害の減少だけでなく、防災システム全体として被害が減少していることを示すことが望ましい。
6.4.2 b)8)	b)8) 供給システムにおける検知された障害等の処理が、b)3)で更新されたゴールに照らして評価されている。	C			障害への対応が適切であったかどうかが、事前に想定したゴールおよび b)3)で更新されたゴールに照らして評価されたことを示すことが望ましい。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.4.2 c)	c) 障害対応が説明責任遂行プロセスビューを用いて説明されている。				
6.4.2 c)1)	c)1) 供給システムの障害による被害への補償が、合意に基づいてなされている。	C			自治体の発災時対応業務において、補償等の必要性があるかどうかを調査しておくことが望ましい。
6.4.2 c)2)	c)2) 供給システムへの信用が持続している。	C			（対応レベルCとしたが、実際に供給システムを実施したことがないと思われるため、現状では判断できない）
6.4.2 c)3)	c)3) 供給システムの障害対応への説明情報がステークホルダ及び一般社会に対して提供されている。この情報には以下が含まれる。 i) 前もって同定した故障等のリストが適切であったことの説明 ii) 検知された故障等の処理が適切であったことの説明 iii) 検知された故障等の重要度解析及び影響分析の結果	C			発災後に、i)ii)iii)によって示された情報が、発災時業務のステークホルダおよび、市民に対して提供できるよう準備することが望ましい。
6.4.2 c)4)	c)4) 説明責任遂行プロセスビューに対して必要な情報が提供されている。	C			発災後に市民に対して説明責任を遂行するために必要な情報を整理し、それが提供できるよう準備することが望ましい。
6.4.2 d)	d) 障害対応ののち、起きた障害の経験に基づき、変化対応プロセスビューを用いて、システムライフサイクルが改善されている。				
6.4.2 d)1)	d)1) 供給システムのライフサイクルの改善のゴールが定義されて合意されている。	B	1-1-1(2)ウ	東日本大震災によって判明した課題に対応するための重点対策が記載されている。これは、平塚市の障害に基づくものではないが、防災システム全体の「改善のゴール」にあたる。	防災システム全体だけでなく、供給システムについても、改善のゴールが詳細化されていることが望ましい。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.4.2 d)2)	d)2) 変化対応プロセスビューに対して必要な情報が提供されている。	C			障害が発生した際に、その結果が全体システムの更新につながるよう情報提供がなされる仕組みについて記述することが望ましい。
6.5.2 a)	変化対応プロセスビュー				
6.5.2 a)	a) 変化が認識、同定されている。				
6.5.2 a)1)	a)1) 環境、前提、リスクなどの、供給システムの適応を必要としうる変更が同定されている。	B	1-2,3	地震被害(1-3)は、「供給システムの適応を必要としうる変更」のうち、リスクにあたる。また、市の概況(1-2)は、環境・前提にあたる。	どの地震被害が供給システムに影響するかなど、防災システム全体だけでなく、各システムごとに適応が必要な変更が分類されることが望ましい。
6.5.2 a)2)	a)2) 予期しない事象（予見されなかった障害を含む）を検知した時に、その原因となった変化が同定される。この同定は障害対応プロセスビューによって引き起こされる場合もある。	C			予期しない事象を検知した際に、その原因となる変化を同定するための体制について記述することが望ましい。
6.5.2 a)3)	a)3) 破壊的な変化は認識され、管理される。	B	4-18	4 章 18 節で定義される「二次災害」とは、発災時の防災業務における「破壊的な変化」であると考えられる。	二次災害に関する記述は左以外にもあるが、現状何を二次災害と想定し、管理しているかが明記されることが望ましい。また、それらと供給システム等との対応関係を明記することが望ましい。
6.5.2 b)	b) 適応が準備されている。				
6.5.2 b)1)	b)1) 変化が供給システムの「目的にかなった」状態に与える影響が評価され、変化と影響の関係が記録されている。	C			例えば、被害想定の見直しのどの部分の変化が、食料の備蓄（影響）に関係しているか、といった対応を洗い出し、記録することが望ましい。
6.5.2 b)2)	b)2) 供給システムの「目的にかなった」状態を維持するための適応のゴールが定義されている。これには以下が含まれる。 i) ステークホルダは、適応の必要、適応の選択肢とそれらの影響などの情報を得ている。 ii) ステークホルダは、変化後の状況でも合意形成の交渉に関して必要な支援を得ている。 iii) 障害対応プロセスビューによって開始される適応によって、障害の再発が防止されている。 iv) 適応のゴールが定義されている。	B	3-8	適応とは、発災時の想定が変化した際に、準備をすることにあたる。すなわち、「今後の取り組みの方向」は、iv）適応のゴール　にあたる。	i)ii)iii)に対応する事項を整理して記述することが望ましい。また、3 章については、防災業務の各システム単位で記述がなされるほうが理解しやすいと考えられる。

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.5.2 b)3)	3) 適応のゴールが合意され、合意文書がそれを反映させて更新される。そのためには合意形成プロセスビューが起動される。	B	1-5-2	防災計画が点検され、更新されるという記述は、合意文書（防災計画）の更新を示す。	合意形成 b)2)でも記したように、防災計画全体だけでなく、各個別のシステムの適応のゴールについて、担当者レベルで合意していることを記録することが望ましい。
6.5.2 c)	c) 適応が遂行される。				
6.5.2 c)1)	c)1) 必要な適応に技術的支援が得られる。	B	3-8, 4-9-1(5)	各項目において、関係機関の支援を得て対策がなされていることが記述されている。	どの適応（変化への対応）に対して、どの機関が支援しているのかが表で整理して記述されることが望ましい。
6.5.2 c)2)	c)2) 過去の経験による知識が効果的に用いられている。	B	1-1(2)イ(ウ)	東日本大震災によって判明した課題に対応するための重点対策は「過去の経験による知識」にあたる。	各重点対策が、地域防災計画のどの記述に反映されたのかを当該箇所で明示するほうが、よりわかりやすい。
6.5.2 c)3)	c)3) ゴールを実現する適応が定義されている。	B	3-8, 4-9	4章9節に定義される業務は、3章8節で定義された「ゴール」を何らかの形で実現していると考えられる。	ゴールを確かに実現しているということが、アシュランスケース等で示されることが望ましい。（ゴールを分割したサブゴールにあたる）
6.5.2 c)4)	c)4) 適応後のサービスが開発される。	B	3-8, 4-9	4章9節に定義される業務は、3章8節で定義された「ゴール」を何らかの形で実現したサービスと考えられる。	ゴールを確かに実現しているということが、アシュランスケース等で示されることが望ましい。（上で記述したサブゴールのソリューションにあたる）
6.5.2 c)5)	c)5) 旧来のサービスの運用中断及び連結した外部供給システムの中断が最小になるよう、適応後のサービスが展開される。	C			（本項目は、常時運用しているシステムを想定した記述なので、防災システムのように、普段はサービスを提供していないものには該当しないと考えられる）
6.5.2 d)	d) 適応後の供給システムが、適応の目的に照らして評価される。	C			防災計画の修正結果が、修正された適応の目的に対して評価され、記録されることが望ましい。
6.5.2 e)	e) 供給システムライフサイクルの改善が不断に続く。	A	1-5-2	防災計画が点検され、更新されるという記述は、ライフサイクルの改善が続くことを示す。	--
6.5.2 f)	f) 説明責任遂行プロセスビューを起動させて、適応の説明がなされる。				

ID	Outcome の平塚市発災時供給システムでの解釈	対応度	対応証拠の記述箇所	対応する理由	現状ないが必要な証拠の記述
6.5.2 f)1)	f)1) 環境その他の変化から適応作業へのトレーサビリティが維持されている。	C			被害想定のどの部分が変化したら（環境その他の変化）、防災計画のどの部分を見直す（適応作業）、ということの対応表を作成することが望ましい。例えば、供給システムの記述を見直すのは、何が変化したときなのかが明示されることが望ましい。
6.5.2 f)2)	f)2) 適応の過程と結果に関する説明が、ステークホルダ及び社会一般に対して提供される。	B	パブリックコメント実施時の、改訂の概要	地域防災計画改訂の説明（適応の過程と結果に関する説明）が、市民（ステークホルダ及び社会一般）に対して提供されている。	上記で作成した対応表に従って、供給システムなど、各システム単位で改訂内容が一覧できることが望ましい。

参照文献

[1] ISO/IEC JTC 1/ SC 7, ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes, International Organization for Standardization, 2015.

[2] International Council on Systems Engineering, INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Edition, Hoboken: John Wiley & Sons, Inc., 2015.

[3] オックスフォード大学出版局, Oxford Advanced Learner's Dictionary オックスフォード現代英英辞典 第 9 版, 旺文社, 2015.

[4] ISO/IEC JTC 1/ SC 7, ISO/IEC 15026-1:2013 Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary, International Organization for Standardization, 2013.

[5] N. Mansourov , D. Campara, System Assurance: Beyond Detecting Vulnerabilities, The MK/OMG Press, 2010.

[6] ISO/IEC JTC 1/ SC 7, ISO/IEC 15026-4:2011 Systems and software engineering -- Systems and software assurance -- Part 4: Assurance in the life cycle, International Organization for Standardization, 2012.

[7] IEC TC56 PT4.8, IEC 62853 Open systems dependability (unpublished Committee Draft for Vote), International Electrotechnical Commission, 2017.

[8] ISO/IEC JTC 1/ SC 7, ISO/IEC/IEEE DIS 24748-2 Systems and software engineering -- Life cycle management -- Part 2: Guidelines to the application of ISO/IEC/IEEE 15288 (System life cycle processes), International Organization for Standardization, 2017.

[9] ISO/IEC JTC 1/ SC 7, ISO/IEC 15026-2:2011 Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case, International Organization for Standardization, 2011.

[10] R. Bloomfield , P. Bishop, "Safety and Assurance Cases: Past, Present and Possible Future - an Adelard Perspective," *Proceeding of the Eighteenth Safety-Critical Systems Symposium*, Bristol, UK, 2010.

[11] M. Tokoro (Ed.), Open Systems Dependability: Dependability Engineering for Ever-Changing Systems, 2nd edition., Boca Raton: CRC Press, 2015.

[12] Origin Consulting (York) Limited, “GSN Community Standard Version 1,” 2011. URL: http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf. [2018-01-13 閲覧].

[13] Adelard, “Safety Case Structuring: Claims Arguments and Evidence,” URL: https://www.adelard.com/asce/choosing-asce/cae.html. [2018-01-13 閲覧].

[14] C. M. Holloway, “Safety Case Notations: Alternatives for the Non-Graphically Inclined?,” *3rd International Conference on System Safety*, Birmingham, 2008.

[15] M. Takeyama, “Chapter 6. D-Case Integrity Checking Tool and Formal Assurance Case,” *Open Systems Dependability: Dependability Engineering for Ever-Changing Systems* , Boca Raton, CRC Press, 2015, pp. 98-125.

[16] Y. Kinoshita , M. Takeyama, “Assurance case as a proof in a theory: towards for mulation of rebuttals,” *Assuring the Safety of Systems - Proceedings of the Twenty-First Safety-critical Systems Symposium,* pp. 205-230, 2013.

[17] 小野寛彬, 情報科学における論理, 日本評論社, 1994.

[18] J. R. Shoenfield, Mathematical Logic, Reprinted Edition, Boca Raton: CRC Press, 2010.

[19] Agda Team, “The Agda Wiki,” URL: http://wiki.portal.chalmers.se/agda/pmwiki.php. [2018-01-13 閲覧].

[20] haskell.org, “Haskell language,” 2017. URL: https://www.haskell.org/. [2018-01-13 閲覧].

[21] Free Software Foundation, Inc., “GNU Emacs,” 2017. URL: https://www.gnu.org/software/emacs/. [2018-01-13 閲覧].

[22] ISO/IEC JTC 1/ SC 7, ISO/IEC/IEEE 15289:2017 Systems and software engineering -- Content of life-cycle information items (documentation), International Organization for Standardization, 2017.

[23] 社団法人 日本情報システム・ユーザー協会(JUAS), ビジネス情報システム開発のための 5W4H で解き明かすプロジェクト管理 ～ここまでやれば成功する, 社団法人日本情報システム・ユーザー協会, 2011.

[24] A. Stretton, “Adding value to project clients,” *PM World Journal*, Vol. V, Issue XII, pp. 1-13, 2016.

[25] 渡邉光太郎, シンプルに結果を出す人の　5W1H 思考, すばる舎, 2017.

[26] J. Zhang , M. L. Huang, “5Ws Model for Big Data Analysis and Visualization,” *2013 IEEE 16th International Conference on Computational Science and Engineering*, Sydney, NSW, Australia, 2013.

[27] D.-Y. Kao, S.-J. Wang, A. Sharma , F. F.-Y. Huang, "A Case-Oriented Model of Digital Forensics on Infected Zombie Computers," *2nd International Conference on Computer Science and its Applications, 2009. CSA '09.*, Jeju, Korea (South), 2009.

[28] J.-D. Kim, J. Son , D.-K. Baik, "CA5W1HOnto: Ontological Context-Aware Model Based on 5W1H," *International Journal of Distributed Sensor Networks,* Vol. 8, Issue 3, 2012.

[29] Y. Hirose, Y. Sasaki , A. Kinoshita, "Human Resource Assignment and Role Representation Mechanism with the "Cascading Staff-Group Authoring" and "Relation/Situation" Model," *Studies in health technology and informatics,* Vol. 84, pp. 740-744, 2001.

[30] K. S. Hwang, K. M. Lee , W.-J. Kim, "Task manifestation-based clinical protocol specification for ubiquitous healthcare services," *IEEE 23rd International Symposium on Computer-Based Medical Systems (CBMS)*, Perth, WA, Australia, 2010.

[31] S. Chung, D. Won, S.-H. Baeg , S. Park, "Service-Oriented Reverse Reengineering: 5W1H Model-Driven Re-Documentation," *IEEE International Conference on Service-Oriented Computing and Applications (SOCA), 2009*, Taipei, Taiwan, 2009.

[32] J. Patton, 川口恭伸 (監訳), 長尾高弘 (訳), ユーザーストーリーマッピング, オライリー・ジャパン, 2015.

[33] Object Management Group, "Business Process Model and Notation (BPMN) Version 2.0," URL: https://www.omg.org/spec/BPMN/2.0/PDF. [2018-01-13 閲覧].

[34] Object Management Group, "OMG® Unified Modeling Language® (OMG UML®) Version 2.5.1," URL: https://www.omg.org/spec/UML/2.5.1/PDF. [2018-01-13 閲覧].

[35] 独立行政法人 情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター 編, 共通フレーム 2013 ～経営者, 業務部門とともに取り組む「使える」システムの実現～, 独立行政法人 情報処理推進機構, 2013.

[36] ISO/IEC JTC 1/ SC 7, ISO/IEC 12207:1995 Information technology -- Software life cycle processes, International Organization for Standardization, 1995.

[37] 内閣府, "日本の災害対策," 2015. URL: http://www.bousai.go.jp/1info/pdf/saigaipamphlet_je.pdf. [2018-01-13 閲覧].

[38] 総務省, "災害対策基本法," URL: http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=336AC0000000223. [2018-01-13 閲覧].

[39] 神奈川県, "地震被害想定調査," 2015. URL: http://www.pref.kanagawa.jp/cnt/f5151/p15579.html. [2018-01-13 閲覧].

[40] 平塚市防災会議, "平塚市地域防災計画 地震災害対策計画," 2015. URL: http://www.city.hiratsuka.kanagawa.jp/bosai/page-c_01661.html. [2018-01-13 閲覧].

[41] IEC TC 1, IEC 60050-192:2015 International electrotechnical vocabulary – Part 192: Dependability, International Electrotechnical Commission, 2015.

[42] I. Sommerville, T. Storer , R. Lock, "Responsibility Modelling for Civil Emergency Planning," *Risk Management,* Vol. 11, pp. 179-207, 2009.

[43] I. Sommerville, R. Lock, T. Storer , J. Dobson, "Deriving Information Requirements from Responsibility Models," *Advanced Information Systems Engineering. CAiSE 2009. Lecture Notes in Computer Science,* Vol. 5565, 2009.

[44] B. Nordström, K. Petersson , J. M. Smith, "Programming in Martin-Löf's Type Theory," 1990. URL: http://www.cse.chalmers.se/research/group/logic/book/. [2018-01-13 閲覧].

[45] 平塚市防災会議, "平塚市地域防災計画 資料編," 2015. URL: http://www.city.hiratsuka.kanagawa.jp/bosai/page-c_01661.html. [2018-01-13 閲覧].

謝辞

本研究は、著者が神奈川大学大学院理学研究科情報科学専攻博士後期課程に在籍した3年間と、神奈川大学プログラミング科学研究所にプロジェクト研究員として在籍した1年間、計4年間の研究をまとめたものです。

主査であり、博士後期課程の指導教官である木下佳樹教授には、終始ご指導ご鞭撻をいただきました。奈良先端科学技術大学院大学の博士前期課程に入学してから 6 年の長きにわたり、著者に対して、熱意あるご指導を頂けたことを、心より感謝申し上げます。物事の本質を掴みとることの大切さを学びました。また、大学院博士後期課程への進学に際して、神奈川大学大学院への進学を勧めて頂いたことを感謝しています。金銭的な不安など色々ありましたが、あの時進学したという判断は正しかったと確信しています。

副査の海谷治彦教授、田中賢教授には、研究の諸段階における学内発表で、有益なコメントを頂きました。深く御礼申し上げます。

副査の産業技術総合研究所・渡邊宏博士には、論文に対して細部にわたり有益なコメントを頂きました。深く感謝申し上げます。

リサーチ・アシスタントとして 3 年間、プロジェクト研究員として 1 年間の計 4 年間在籍している神奈川大学プログラミング科学研究所の皆様に、深く感謝申し上げます。武山誠博士には、博士後期課程の 3 年間、アドバイザーとして研究に対して様々なコメントを頂きました。中原早生博士及び奥野康二氏には、同僚として、人生の大先輩としてご指導ご鞭撻を頂きました。研究補助員の松本佳子さんには、公私にわたり様々なサポートを頂きました。お名前を記して心より御礼申し上げます。

本論文の事例研究は、平塚市との共同研究「平塚市地域防災計画の整合性検査方式の研究」の成果です。平塚市防災危機管理部災害対策課の皆様に感謝申し上げます。特に、長きにわたり定例の打合せに参加いただき、さまざまなコメントを頂戴しました近藤康裕、須藤圭祐両氏に、お名前を記して御礼申し上げます。

著者は 2016 年秋より ISO/IEC JTC 1/SC 7/WG 7 の国内委員会（情報処理学会 情報規格調査会）に所属し、委員会での議論を行うことで、本論文が扱う国際標準群への理解を深めることができました。WG 7 委員会の皆様に厚く御礼申し上げます。

本研究の一部は、独立行政法人情報処理推進機構（IPA）が実施したソフトウェア工学分野の先導的研究支援事業(RISE)「オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク」の支援を受けました。深く御礼申し上げます。

今の私があるのは、幼い頃からの教育と、コンピュータに触れる環境があったお陰です。そんな環境を提供してくれた父・裕三と、母・敦子に感謝します。また、切磋琢磨して育ち、博士後期課程進学の際は半年間東京・月島にて寝食を共にした兄・祐馬に感謝します。

最後に、結婚後に会社を退職して大学院に進学した無鉄砲な私を根気強く支えてくれた妻・紫野と、日々に癒しと気づきを与えてくれる娘・花に深甚なる感謝の意を表します。

発表リスト

末尾の括弧内に、本論文で主に対応する箇所を示した。

1. S. Kinoshita, Y. Kinoshita, “The 6W1H Model as a Basis for Systems Assurance Argument,” *Computer Safety, Reliability, and Security. SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, Trondheim, Norway, September 20, 2016, Proceedings, Lecture Notes in Computer Science*, Vol. 9923, Springer, pp.63-74, 2016.09. （4 章と 5.1 節～5.3 節）
2. 奥野康二, 木下修司, 木下佳樹, 武山誠, 中原早生,“オープンシステム・ディペンダビリティのための形式アシュランスケース・フレームワーク(FFO)”, *IPA SEC journal*, Vol. 13 No. 2, pp.44-51, 2017.09. （5.4 節）
3. S. Kinoshita, Y. Kinoshita, “A Thought Experiment on Evolution of Assurance Cases - from a Logical Aspect,” *Computer Safety, Reliability, and Security. SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings, Lecture Notes in Computer Science*, Vol. 10489, Springer, pp.17-26, 2017.09. （3.3 節）