学位報告 4

報告番号	※甲　　第　　号

主　論　文　の　要　旨

論文題目

アクター概念に基づくアシュアランスケース設計法に関する研究

氏　　名　猿渡　卓也

論 文 内 容 の 要 旨

社会における様々な分野で IT 技術が利用されている．金融システムや交通システム等の社会的に重要なインフラや，医療分野等の人の生命に直接関わる分野においても，IT 技術は不可欠な存在となってきている．このような重要な分野におけるシステムの障害は大きな損失をもたらし，社会的な問題となる．また，近年のシステムの多くには，システムが独立に存在しているのではなく，システム同士が相互に連携しているという特徴がある．複数のシステムが相互に連携しているという状況が，この問題の解決をさらに難しくしている．このような状況の中で，システムのディペンダビリティや安全性等を保証する技術として，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や安全性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することができる．アシュアランスケースの使用により，システムのディペンダビリティや安全性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可能となる．ステークホルダによるシステムのディペンダビリティや安全性に関する議論の共有は，システムやシステムを利用したサービスの保証につながる．しかしながら，従来の研究において提案されているアシュアランスケースの記法には，次の 3 つの欠陥が存在する．欠陥①：複数のシステムや複数のコンポーネントから構成されるシステムの保証が考慮されていない．欠陥②：アシュアランスケースで実施される議論を保証する責任主体の概念が考慮されていない．欠陥③：アシュアランスケースと既存の設計手法との関係が不明確である．本研究では，これら 3 つの欠陥に対して，次の 3 つの課題を設定し，研究を実施する．課題①：複数の要素から構成されるシステムを保証するためのアシュアランスケースの提案．課題②：アシュアランスケースに対する責任属性の導入．課題③：アシュアランスケースと既存の設計手法の関係の明確化．以下では，本研究において，上記課題に対して実施した研究について述べる．

“課題①：複数の要素から構成されるシステムを保証するためのアシュアランスケースの提案”では，複数の要素から構成されるシステムの保証について，アシュアランスケースを使って記述できるように，従来から提案されているアシュアランスケースの記法を拡張する．近年，単独で存在するシステムは少なくなってきており，相互に連携するシステムが増加してきている．このようなシステムは，System of systems（SoS）の概念でも知られている．また，1 つのシステムに着目すると，システム自体が複数のコンポーネントから構成されている場合が多くなってきている．すなわち，現状において構築されているシステムの多くは，複数のシステムやコンポーネントが相互に依存する構成となっている．このような状況であるにも関わらず，従来のアシュアランスケースには，複数のシステムやコンポーネントから構成されるシステムの保証が考慮されていないという欠陥が存在した．従来のアシュアランスケースでは，対象のディペンダビリティや安全性に関する議論を，基本的に全て 1 つのアシュアランスケースに記述する．これは，システムが複数の要素から構成されている場合でも同様である．従来のアシュアランスケースでは，アシュアランスケースの中で，システムの複数の構成要素を表現する手段が無い．これでは複数のシステムやコンポーネントが相互に依存するシステムの保証に関する議論を記述することは難しい．すなわち，従来のアシュアランスケースには，複数のシステムやコンポーネントが相互に依存するシステムの議論を，効率的に実施できるようにするという課題がある．本研究では，この課題に対する取り組みとして d* framework を提案する．d* framework とは，Actor の概念を導入したアシュアランスケースの作成手法である．また，d* framework を使用して作成されたアシュアランスケース自体も d* framework と呼ばれる．本研究において，d* framework は，アシュアランスケースの代表的な記法の 1 つである GSN を拡張して定義された．d* framework では，GSN で使用されている要素に加えて，Actor が新規の要素として追加されている．Actor は d* framework が対象とするシステムの構成要素を示す要素として使用される．システム，サブシステム，コンポーネント，人，組織等を Actor として定義することができる．d* framework を使用し，システムやシステムを構成するコンポーネントを Actor として定義することにより，複数のシステムや複数のコンポーネントから構成されるシステムの保証を明確に示すことができるようになると考えられる．

また本研究では，提案した d* framework について，適用実験に基づく評価を実施した．適用実験では，SIer で使用されている IT システムを使ったサービスを対象として，実際に d* framework を作成することで，d* framework の評価を実施した．d* framework の作成に伴うステークホルダの負担を軽くするため，対象のサービスに直接関係していない第三者が中心となって d* framework を作成した．対象のサービスに直接関係していない第三者が，対象サービスの d* framework を作成することは困難である．そこで，本研究では，第三者による d* framework の作成手順を定義し，その手順を使用して d* framework を作成した．また，作成には対象サービスに関連する文書を使用した．その結果，132 個の要素を持つ d* framework が作成された．作成された d* framework は，ステークホルダから見ても違和感のないものとなった．また，本研究では，作成された d* framework を使って，ディペンダビリティに関する議論の漏れを確認する実験も実施した．議論の漏れの確認には，d* framework が持つ構造的な特徴を利用した．その結果，全体で 45 個の議論の漏れを特定することができた．また，d* framework の適用可能性を評価するため，対象としたサービスのステークホルダに対して，本研究で実施した取り組みに関するヒアリングを実施した．その結果，d* framework を作成することでサービスのディペンダビリティに関する議論を分かりやすく整理することができ，対象サービスを考慮すれば d* framework を実際に活用できるという評価が得られた．この結果より，d* framework は，実際の現場においても利用価値のあるものであることが示された．また，本研究を実施したことに

より，サービスに直接関係していない第三者でも d* framework の作成が可能であることが示された．

“課題②：アシュアランスケースに対する責任属性の導入”は，アシュアランスケースで実施される議論を保証する責任主体の概念が考慮されていないという，従来のアシュアアンスケースが持つ欠陥に対応した課題である．アシュアランスケースには，システムを保証するための議論が記述される．アシュアランスケースに記述される議論により，対象のシステムが保証されるためには，アシュアランスケースに記述される議論そのものが保証される必要がある．そのためには，アシュアランスケースに記述される議論そのものに責任を持つ責任主体が，明確になっている必要がある．しかし，従来のアシュアランスケースでは，必ずしもこの責任主体を明示的に記述することができなかった．つまり，従来のアシュアランスケースには，アシュアランスケースで実施される議論を保証する責任主体の概念が考慮されていないという欠陥が存在する．本研究では，この課題に対する取り組みとして，d* framework に対して，新規の要素である Agent を導入することを提案する．Agent は，d* framework において実施されている議論に対して責任を持つ責任主体を示す要素として定義される．すなわち，Agent として定義された要素は，d* framework 内の他の要素（Actor，Goal，Strategy，Context，Evidence）に対して責任を持つ．そのため，Agent として定義できるのは，議論に対して責任を持つことができる人や組織等であるとした．逆に，それ自体では責任を持つことができないシステムやサブシステム等は，Agent として定義することはできないとした．本研究において，d* framework に Agent の要素を導入したことで，d* framework で実施される議論を保証する責任主体の概念を考慮することができるようになったと考えられる．

“課題③：アシュアランスケースと既存の設計手法の関係の明確化”では，d* framework と既存の設計手法の 1 つであるコラボレーション図の関係を明確にする．さらに，コラボレーション図を使った d* framework の作成手法を提案する．アシュアランスケースは，ソフトウェア工学の分野における手法の 1 つである．ソフトウェア工学の分野では，システム開発の上流工程から下流工程に至る様々な工程を対象として，システム開発を行うための研究が実施されている．それらの研究において，システム開発で使用できる様々なモデルが提案されている．これらのモデルとアシュアランスケースの間には関係があると考えられる．また，この関係を明らかにすることで，アシュアランスケースをより効果的に使用することができるようになると考えられる．しかし，アシュアランスケースとそれら既存の設計手法との関連に関する研究は，ほとんど存在しない．すなわち，既存のアシュアランスケースに関する研究には，アシュアランスケースと既存の設計手法との関係が不明確であるという欠陥が存在する．本研究において，既存の設計手法のモデルであるコラボレーション図と d* framework（アシュアランスケース）の関係を明らかにすることにより，既存の設計手法の 1 つとアシュアランスケースの関係を明らかにすることができた．

上記に示す通り，本研究では，アシュアランスケースの記法である d* framework を使って，アシュアランスケースの研究における 3 つの課題に対する研究を実施した．