演習コースⅡ 形式手法と仕様記述（第３グループ）

形式仕様記述言語の利用による仕様書の改善
—USDMと形式仕様記述の考察を通して—

Improvement of Specifications by Formal Specification Language
- Through Consideration of USDM and Formal Specification Description-

宮本　陽子　　株式会社メタテクノ

概要

本研究では，USDMにおける自然言語による仕様の記述に対する注意点がIEEE 830の品質特性とどのような関係性を持つかについて整理するとともに，自然言語記述の場合と比較して，形式仕様記述手法（VDM）を利用する場合の利点について考察する．これらの整理・考察の結果，仕様書の品質を向上させる方法の一つとして，USDMに則った仕様記述においてVDMを併用することが，仕様書の厳密性，無矛盾性，変更容易性を高めることに有効であることを示す．

Abstract

In this research, the guideline for natural language specification shown in USDM is classified, in terms of quality criteria defined in IEEE 830. Compared with natural language specification, a formal specification method (VDM) is considered more advantagenous. When VDM is used together with USDM as one of the methods to improve quality of specifications, VDM is considered effective to improve unambiguity, consistency and modifiability.

1. はじめに

1.1 開発における要求仕様策定の問題

著者の所属する開発現場では，要求仕様書（以下，仕様書）に起因する欠陥が上流工程で検出できず，このことが手戻りによる工数増加やスケジュールの遅延につながる場合もあるため，仕様書の品質向上が重要な課題となっている．仕様書に起因する欠陥を上流工程で検出しきれず，後続の工程に先送りしてしまう原因はいくつかあると考えられ，現場での議論では，次のことが挙げられた．

- ●仕様書レビューを行っても，良い仕様書の書き方に対する理解がなく，誤字脱字の指摘しかでない．
- ●仕様書がどのような品質になれば仕様策定完了なのか，明確な基準がない．
- ●仕様記述があいまいで，設計者は経験から理解しているが，テスト工程で第三者が読

むと不明点が見つかる．

これらから，良い仕様書の書き方に対する組織的な共通認識，仕様策定における基準やガイドラインの必要性を感じた．

1.2 良い仕様書に関するこれまでの知見

既に，良い仕様書の書き方に関し参考になる知見として，例えば，IEEE 830-1998[1]（以下，IEEE 830）と USDM （Universal Specification Describing Manner）[2]がある．

IEEE 830 とは，IEEE が定めた，ソフトウェア要求仕様書を記述する際に参照するための規格である．大西らは，「この規格に準拠することにより，品質の高い要求仕様書（良い要求仕様書）が作成できる」[3]とし，IEEE 830 では，良い仕様書が満たすべき品質特性（以下，品質特性と称する）として，以下をあげている[3]．

a) 妥当であること
b) あいまいでないこと
c) 完全であること
d) 矛盾がないこと
e) 重要度と安定度のランク付けがされていること
f) 検証可能であること
g) 変更が容易であること
h) 追跡可能であること

USDM とは，自然言語（日本語）の要求文から，動詞と目的語に着目して仕様をとらえることや，要求を分割・階層化し，要求仕様・理由・説明をセットにした表形式で仕様書を記述・管理することなどを，具体例を交えて提案したものである[2]．

一方，良い仕様・文を書くための手法として，形式手法 VDM ，形式仕様記述言語 VDM++ があり，日本国内では，最近特に注目されている．

形式手法とは，数理論理学に基づく科学的な裏付けを持つ言語を用いて設計対象の機能や性質を表現することにより，ある側面の仕様を厳密に記述し，開発工程で利用する手段の総称[4]であり，VDM (Vienna Development Method) は，モデル規範型に属する手法の一種である．形式仕様記述言語 VDM++ は，ISO で標準化されている VDM-SL (VDM Specification Language)に対して，主にオブジェクト指向の拡張を行った言語であり，これにより，様々な抽象度で，モデリングから仕様記述までを，大規模，広範囲に行うことができる[5]．VDM++ には，命題論理，述語論理，集合，写像といった数理論理や，抽象データ型を表現する記法があり，これらを用いて，モデルの状態とそれらの不変条件，事前条件，事後条件の記述を行うことができる．これにより，コンパクトな仕様の記述，仕様の検査によるあいまいさの除去，仕様の実行，テスト，回帰テスト等が可能となる[4][5]．

1.3 目的

IEEE 830 の規格や USDM の手法，形式仕様記述手法 VDM は，どれも品質の高い仕様書（良い仕様書）を作成するためのものであるが，相互の関係性が不明で，何をどのように活用すべきか，一般的には明らかになっていない．そのため，本研究では，IEEE 830 の品質特性と USDM ，VDM との関係を整理し，何がどの観点で仕様書の品質向上に寄

与するかを調査することとした．

本論文の構成は，以下のとおりである．2 章で本研究の方法について，3 章で方法に対する結果，4 章で注目すべき結果とその考察，得られた知見について述べる．

2. 方法

本研究は以下の手順で行った．

(1) USDM から自然言語の仕様記述に対する注意点を集めるため，「すべし」・「すべからず」の形式で洗い出す．なお，本研究の対象を「仕様記述」としたため，USDM に含まれる要件管理・計測などは対象外となった．

(2) USDM と IEEE 830 の品質特性との関係性を明らかにするため，(1)で洗い出した USDM の主要な注意点が，IEEE 830 の品質特性の何と関連するかを整理する．

(3) IEEE 830 の品質特性と自然言語，VDM の関係性を明らかにするため，(1)で洗い出した注意点に対し，自然言語のみで記述する場合と比べ，VDM を組み合わせて利用する場合の効果と課題を検討しながら，以下に分類する．

① VDM を用いると自然言語よりも解決が容易になるもの
② VDM を用いても解決が容易にならないもの
③ どちらとも言えない（直接大きな効果があるわけではないが，関連があるもの）

3. 結果

手順(1)で洗い出した結果，USDM の自然言語の仕様記述に対する注意点が，51 個列挙できた．手順(2)・(3)の結果をまとめると，下記，表 1 のとおりとなった．表 1 の 1 番左の列は，IEEE 830 の品質特性で，その隣の列に簡単な説明を付している．また，USDM の自然言語仕様に対する注意点を，手順(2)で関連づけた品質特性の右横に記した．さらに，手順(3)の分類結果と理由を一番右に示した．なお，紙面の都合上，表 1 には代表的な①，②のみ抜粋し，③については 4 章の本文で一例を取り上げる．更に，表 2 に，手順(2)・(3)で整理・分類した個数をまとめた．

表 1. 品質特性と各手法の関係表（抜粋）

IEEE 830 の品質特性	品質特性の説明	USDM の自然言語仕様に対する注意点	自然言語と VDM との組み合わせ時	
			分類	分類理由
a) 妥当であること	顧客やユーザのニーズと一致していること．上位のシステム要求仕様書などの関連する他のドキュメントとの矛盾がないこと	未確定項目がある場合は，どのように合意するか，依頼者と合意形成方法を決めておくべし	②	プロセスに対しての注意点であるため，VDM による効果は見込めない．
b) あいまいでないこと	要求仕様書に記述されている要求が，ただ一通りに解釈できること	要求仕様書の"善し悪し"を判断する手段や基準をもつべし	①	VDM では仕様テストにより善し悪しを判断できるため
		「範囲」を読み取れるように要求を表現すべし	①	VDM 記述時に自然と範囲を考えるため 不変・事前・事後条件の記載により意識するため

		仕様は「仕様である」ことを明示して記述し， 説明は「説明である」ことを明示して記述すべし	①	VDM で「要求」を，自然言語でコメントとして「理由」を記載することにより，記述形式を分けられるため
		要求仕様書では，記述内容が″Specify″，すなわち″特定″できる表現になっているものを″仕様″とすべし（″仕様″の定義）	①	VDM の仕様記述とテストケースの記述により，関係者間で合意しやすくなるため
		要求仕様書の構成や内容は，後工程の読者にわかるように書くべし	①	文法・意味論が定まっているため，記述されたことに対して一意に読み取れるようになっているため
		「等」や「etc」をできるだけ使わないようにすべし． 使う場合は，○月○日までに決めるとコメントをつけるべし．	①	VDM では「等」「etc」があると仕様記述ができないため
c）完全であること	顧客やユーザの，情報システムに対するニーズが漏れなく要求仕様書に記述されており，かつ図表の参照や用語の定義などの，要求仕様書の形式が整っていること	「境界」は早い段階で決めるべし	①	VDM では外部 I/F に限らず，責務が明確になるため．陰仕様で書くだけで「決まった」かどうかが，明示的にわかるため
		「要求」のモレを防ぐために， カテゴリの分割や要求の分割・階層化に漏れがない，隙間がないことを確認できるようにすべし	①	VDM では，仕様のテストが可能なため，要求のレベルでテストできるため． 場合分け，例えば if then else や，cases に対する others など一部の種類の分割には VDM のほうがモレをチェックしやすいため
		要求仕様書には「品質要求」を記載すべし	②	VDM で「操作性」「保守性」「交換性」などの品質要求を記述するのは困難なため
		階層化の基準として，以下を(状況によっては組み合わせて)使い，「隙間」なく分割すべし ・時系列分割（時間軸分割） ・構成分割 ・状態分割 ・共通分割	①	VDM で書く際に分割・階層化を意識せざるを得ないため VDM でテストを行えば，「隙間」はエラーとして指摘されるため
		モレなく書くべし	①	VDM ではモレがあると仕様テストが実行できないなど，気づきやすいため
		要求仕様の番号をテストケースの番号と交換し，テストケースにモレがないことを確認すべし	①	VDM では仕様テストにより仕様カバレッジが測定できるため，番号の交換をせずともテストケースにモレがあるかどうか確認しやすい
		仕様をグループに分けて，さらに集合を小さくし，できるだけ混じり気のない仕様のグループを作るべし	①	VDM では構造化設計・オブジェクト指向を意識するため，自然とクラス・モジュールによるグループ化を行うため
		<グループ名>に要求の性質を持たせるためには，範囲をあらわしていることを意識してグループ名を選ぶべし．	②	VDM を使う場合も，クラス名や操作名，関数名を決める際は，わかりやすい名前をつけなくてはいけないため，変わらない
		「・・・・・は，・・・・・しない」という「否定表現」を避け， then と else の両方を明らかにすべし	①	VDM では if then else を記載することで強制的に考えるため

d）矛盾がないこと	要求仕様書内部で矛盾や衝突がないこと	ほかの機能の仕様と衝突していることに気づくためにも，仕様は早期に展開すべし	①	VDM では，たとえば，複数の機能が同じ変数を操作している際，競合の可能性があることを機械的に検出することも可能なため 日本語などの自然言語で仕様化した場合は，機械的な検出は難しい
		早い段階で全体の仕様化を行うべし	①	VDM では，動かすために全体を書き出すことになったり，動かしてみて抜けているところに気づいたりしやすいため
e）重要度と安定度のランク付けがされていること	各要求について，重要度と安定度を示す指標を明確につけておくこと	確認中の仕様をそのまま記述し，変わる可能性があることを明記すべし	①	仕様とコメントが分かれているので付けやすいため VDM では，関数・操作の本体に is not yet specified という記法で暫定定義であることを明記できるため
f）検証可能であること	開発されたソフトウェアが，要求仕様書に記述された要求を満たしているかどうかを確認可能であること	検査部門の人に，「検証可能」という側面から要求仕様書のレビューを実施してもらうべし	①	VDM では正しさの条件として，不変条件などの記載があることにより，開発者が他者に説明しやすい．仕様網羅度も基準として有用．また，VDM でテストケースを作成できれば，「検証可能」と言えるため．
		品質要求はテストでも確認すべし	②	VDM で品質要求を記述するのは困難なため
g）変更が容易であること	要求仕様書に対する変更が，容易に，完全に，一貫して行えるようになっていること a)目次や索引，明確な相互参照が整備され，使いやすい構造になっている b)冗長でない．つまり，同じ要求が要求仕様書内で複数個所に記述されていない c)他の要求と混ざらず，各要求を独立・分離して表現している．つまり，要求が互いに依存していない	重複なく書くべし	①	VDM ではコードクローンを発見しやすく，重複に気づいたら構造化設計をしなおすことで解決できるため
		仕様書全体を「均一」に記述することにこだわるべからず 関係者間で共有できている認定仕様まで，詳細に記載しなくてもよい	①	VDMで記述する範囲を決めることと言い換えられ，VDM では関係者間で共有できていることは何か，共有できていないことは何か，が議論できるため
		仕様番号の確定作業は，仕様化の最初の段階では行うべからず．グループ分け確定後に行うべし	①	VDM ではクラス名・操作名などグループ化の観点がわかりやすいため
		似た記述が続く場合に，何が違うかをすぐに読み取れるようにすべし	①	VDM では似たものでも違う場合は明示的に表現するため．例えば，cases とか．
h）追跡可能であること	要求仕様書に記述された個々の要求に関し，その起源が明確であり，開発が進行するに伴って作成された文書等との対応付けがとれること a)後方追跡可能性 b)前方追跡可能性	設計や実装の工程で明らかになった「仕様」は，要求仕様書に書き戻すべし	①	VDM 仕様のクラス名・操作名・関数名と設計・実装の対応が明確になりやすく，迷うことなく書き戻せるから 自然言語仕様ではどこの文に書き戻すべきか探しにくいため
		「要求」と「理由」をセットで表現すべし	①	VDM で「要求」を，自然言語でコメントとして「理由」を記載することにより，記述形式を分けられるため
		要求仕様には固有の記番号を付けるべし	②	VDM では番号づけを強制されない．また，番号をふるのも機械的にはできず，人に依存するため

表 2. 手順(2)・(3)で整理・分類した結果の個数

IEEE 830 の品質特性	USDM 注意点個数	VDM との組み合せ時		
		①	②	③
a) 妥当であること	2	0	1	1
b) あいまいでないこと	9	9	0	0
c) 完全であること	18	13	5	0
d) 矛盾がないこと	3	3	0	0
e) 重要度と安定度のランク付けがされていること	1	1	0	0
f) 検証可能であること	4	3	1	0
g) 変更が容易であること	5	5	0	0
h) 追跡可能であること	5	2	2	1
その他	4	2	2	0
合計	51	38	11	2

凡例
①VDM を用いると自然言語よりも解決が容易になるもの
②VDM を用いても解決が容易にならないもの
③どちらとも言えないもの

4. 注目すべき結果・考察・得られた知見

IEEE 830 の品質特性と USDM について：

注目すべき結果

表１・表 2 より，USDM の自然言語仕様に対する注意点は，IEEE 830 の品質特性の全てに関連していた．

しかし，e)重要度と安定度のランク付けがされていること，に対しては，「確認中の仕様をそのまま記述し，変わる可能性があることを明記すべし」という安定度に関する１つのみで，重要度に関するものはなかった．

考察

上記の結果より，仕様策定時にガイドラインとして USDM の 51 個の注意点を用いることは，仕様書の妥当性，非あいまい性，完全性，無矛盾性，検証可能性，変更容易性，追跡可能性，安定度のランク付け・明示に寄与すると言える．

なお，要求の重要度は，開発費用や期間，要求間の競合により，全ての要求を実現できない場合に，実際に実現する要求を仕様として選択できるようにするために必要である．USDM は手軽に利用できるという位置づけであるため，複雑さを避けるべく，重要度のランク付け・明示を導入していないという可能性はある．また，重要度を考えると，『重要な理由』『その理由が重要な理由』というように，組織のビジョンや戦略まで何階層もさかのぼることになってしまう．このような事情から，仕様化に焦点をあて，手軽にという USDM のフォーカスに合わない点を考慮しているのかもしれない．

得られた知見

要求の重要度を USDM における「理由」に数値でつけるなど，簡単な拡張で重要度を記述することができると考えられる．このような拡張形式を，要求が多く，全てが実現できるか不明な場合に限り用いることも考えられる．さらに， USDM の「理由」の記述に

おいて，その要求が重要である理由を書くようにすることも考えられる．

IEEE 830 は，基準を示すのが目的であるため，要求仕様書を作成する際の特定の手法等については対象外[3]としており，その品質特性は，良い仕様書のあり方を考えるための参考である．それに対して， USDM は， IEEE 830 の全ての品質特性に寄与する，より具体的な基準を提示するものとして有用である．

自然言語のみによる記述と VDM による記述について：

注目すべき結果

表 2 より，USDM の自然言語仕様に対する注意点 51 個のうち，自然言語のみで仕様記述を行う場合に比べ，VDM を用いることで解決が容易になるもの（①）が 38 個で，約 75%を占めていた．言い換えると，残りの 25%については，VDM を用いても解決が容易にならない（②），もしくは，どちらとも言えない（③），に分類されている．

③のどちらとも言えないは，直接大きな効果があるわけではないが，関連があることを意味する．「何に依存して仕様が決まっているかを整理すべし」の注意点を例にすると，仕様の根拠は，開発対象によって，法律や通信規格，それまでの作業習慣，製品で使用される部品の性能など，複数の要素が考えられる[2]．通信規格のように VDM で記述することで効果を見込める場合もあれば，作業習慣のように VDM で記述しにくく効果が見込めない場合もあるため，③の分類とした．

また，表 2 より，IEEE 830 の品質特性の，b)あいまいでないこと，d)矛盾がないこと，g)変更が容易であることに関連する注意点は，全て，VDM を用いることで解決が容易になるもの（①）に分類され，②・③は一つもなかった．

考察

上記の結果より， USDM で挙げている注意点に対しては，自然言語のみの仕様記述よりも，VDM を用いた仕様記述が有効であるものが多いと言える．特に，IEEE 830 の品質特性の非あいまい性，無矛盾性，変更容易性に対しては，VDM は自然言語より優位である．これは，VDM では，ツールによって構文や型を機械的に検査しながら記述できたり，仕様のテストによって不変条件・事前条件・事後条件などの違反を検出できたり，「if 文に対して else 文を必ず明記すること」など，ルール化しやすい点が考えられる．

ただし，VDM を用いても，USDM で挙げている注意点の解決しやすさに効果がないものも少なからず存在する．②・③に分類されたものの多くは，「保守性」や「応答性」，「操作性」などの品質要求に関する注意点であった．

得られた知見：

品質要求には「機能ごとに設定される品質要求」と，製品やシステムの「全体にかかる品質要求」があり，たった一つの品質要求をはずすことで製品としての価値が失せてしまうこともある[2]とされる．

本研究を行う以前は，VDM で仕様書の全てを記述できるのでは，と安易に考えていた．しかし，このように品質要求は重要なものであり，VDM で記述しても効果が見込めない部分であることから，VDM で仕様書の全てを記述するのは避けるべきであろう．

また，IEEE 830 の品質特性との関係から，USDM に則った仕様記述を行う際にも，VDM を組み合わせて利用することで，自然言語のみの場合より，厳密で矛盾のない，変更が容易な仕様書を作成しやすくなるため，VDM の活用を提案したい．

5. おわりに

IEEE 830 の品質特性は，良い仕様書のあり方を提示する抽象的なものである．それに対して，USDM は要求を仕様化する際に守るべき，より具体的な作法（マナー）を示している．さらに，そのマナーは VDM で理論に基づき厳密に記述することで，機械による検証の支援を受けたり，仕様記述のルールを決めたりすることが可能になるため，組織として順守しやすくなる．USDM と VDM を併用することは，IEEE 830 の品質特性の観点から見ても仕様書の品質向上に寄与するため，ソフトウェアの開発現場から手戻りやスケジュールの遅れを減らす可能性があると言える．

謝辞

本論文の執筆に当たり，システムクリエイツの清水吉男氏，九州大学大学院の荒木啓二郎教授，栗田太郎主査，石川冬樹副主査，日科技連・演習コースⅡの研究員の皆さま，日科技連・事務局の皆さま，三森早希子氏にお世話になりました．厚く御礼申し上げます．

参考文献

1 IEEE Recommended Practice for Software Requirement Specifications, IEEE Std 830-1998
2 清水吉男,【改訂第 2 版】[入門＋実践]要求を仕様化する技術・表現する技術～仕様が書けていますか？，技術評論社，2010
3 大西淳・妻木俊彦・白銀純子，トップエスイー基礎講座 2 要求工学概論 要求工学の基本概念から応用まで，近代科学社，2009
4 栗田太郎，モバイル FeliCa のソフトウェア開発における品質確保のための構造と実践 抽象度の制御やコミュニケーションの活性化に向けて，情報処理学会，2010
5 栗田太郎・荒木啓二郎，モデル規範型形式手法 VDM と仕様記述言語 VDM++ －高信頼性システムの開発に向けて―，信頼性，2009