

非機能要求グレード 2018 利用ガイド

[解説編]

2018 年 4 月



独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

非機能要求グレード 2018 利用ガイド[解説編]

2018 年 4 月

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター

©2010-2018 独立行政法人情報処理推進機構

[使用条件]

1. 本資料の著作権は、独立行政法人情報処理推進機構が保有しています。
2. 本資料は著作権法による保護を受けており、本資料の使用者は、本資料の全部または一部を項番3に定める場合を除き、独立行政法人情報処理推進機構の許諾なく無断で改変、公衆送信、販売、出版、翻訳/翻案することは営利目的、非営利目的に関わらず禁じられています。
3. 独立行政法人情報処理推進機構は、本資料の使用者が、以下の著作権表示を明記することを条件として、①及び②の行為を行うことを許諾します。

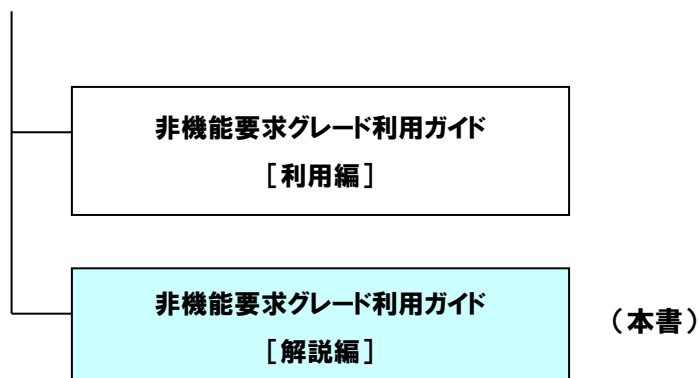
著作権表示：(c)2010-2018 独立行政法人情報処理推進機構

 - ① 資料の全部または一部を複製すること。
 - ② 本ページに記載されている使用条件を配布先に遵守させることを条件に本資料の複製物を無償で再配布すること。
4. 独立行政法人情報処理推進機構は、本資料が第三者の著作権、特許権、実用新案権等の知的財産権に抵触しないことを一切保証するものではなく、また、本資料の内容に誤りがあった場合でも一切責任を負いかねます。
5. 独立行政法人情報処理推進機構は、本ページで記載された許諾内容を除き、独立行政法人情報処理推進機構または第三者の著作権、特許権、実用新案権等の知的財産権に基づくいかなる権利を許諾するものではありません。
6. 独立行政法人情報処理推進機構は、本資料のシステム開発への利用、開発されたシステムの使用、及び当該システムの使用不能等により生じるいかなる損害についても、なんら責任を負うものではありません。
7. 本資料を海外へ持ち出す場合及び非居住者に提供する場合には、「外国為替及び外国貿易法」の規制及び米国輸出管理規則等外国の輸出関連法規を確認のうえ、必要な手続きを行って下さい。
8. 本資料へのお問い合わせについては、独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センターまでご連絡下さい。

非機能要求グレード利用ガイド〔解説編〕とは

非機能要求グレード利用ガイドは、以下の図に示すように、〔利用編〕と〔解説編〕とで構成される。

非機能要求グレード利用ガイドの構成



図． 非機能要求グレード利用ガイド〔解説編〕の位置づけ

本書は、システム基盤の発注者要求が見える化する非機能要求グレードを作成した背景や、ツールの詳細等を解説することを目的としている。

非機能要求グレードの利用方法については、〔利用編〕を参照いただきたい。

なお、「非機能要求グレード」とは、非機能要求グレード利用ガイド、及び以下の3つのツールの総称である。

- 「システム基盤の非機能要求に関するグレード表（以下、グレード表）」
- 「システム基盤の非機能要求に関する項目一覧（以下、項目一覧）」
- 「システム基盤の非機能要求に関する樹系図（以下、樹系図）」

本書の主な対象読者

本書の主な対象読者は、企業の業務システム等、情報システムの開発において、要件定義などの場面で非機能要求を提示、提案、決定することに関わる発注者、受注者双方の担当者である。なお、本書では以後、発注者についてはユーザ、受注者についてベンダと統一して呼ぶこととする。

本書の構成

本ガイドの構成を以下の表に示す。

表. 非機能要求グレード利用ガイド [解説編] の構成

章番号	章題	概要
1 章	はじめに	非機能要求グレード策定の背景やスコープ等について説明する。
2 章	非機能要求グレードの詳細説明	非機能要求グレードの仕様や各大項目について説明する。
3 章	FAQ	非機能要求グレードについてよく聞かれる質問と回答について説明する。
4 章	用語集	非機能要求グレードで使用している用語について説明する。
5 章	付録	他標準との関連等、補足情報を説明する。

目次

1 はじめに	1
1.1 非機能要求グレード策定の背景とねらい	1
1.2 非機能要求の問題と非機能要求グレードの解決方法	4
1.3 非機能要求グレードのスコープ	5
1.3.1 非機能要求の定義とシステム基盤との関係	5
1.3.2 スコープとしている項目	6
1.3.3 スコープ外の項目について	8
1.4 非機能要求グレードの概要	9
1.4.1 非機能要求グレードの基本コンセプト	9
1.4.2 非機能要求グレードの構成要素・概要	10
2 非機能要求グレードの詳細説明	14
2.1 非機能要求グレードの詳細説明	14
2.1.1 グレード表	14
2.1.2 項目一覧	18
2.1.3 樹系図	21
2.2 各大項目の概要と留意事項	22
2.2.1 可用性	22
2.2.2 性能・拡張性	24
2.2.3 運用・保守性	26
2.2.4 移行性	28
2.2.5 セキュリティ	30
2.2.6 システム環境・エコロジー	33
3 FAQ	35
4 用語集	40
5 付録	48
5.1 非機能要求に関する他活動との関係について	48
5.1.1 JUAS「非機能要求仕様定義ガイドライン 2008」との関係	48
5.1.2 JEITA「民間向け IT システムの SLA ガイドライン」との関係	49
5.1.3 IPA/SEC「非機能要求記述ガイド」との関係	49

5.2 他活動との関係について	50
5.2.1 ISO/IEC 9126-1:2001 との関係	50
5.2.2 共通フレーム 2007 との関係	52
5.2.3 情報システムの信頼性向上に関するガイドラインとの関係	52
5.2.4 ISO/IEC 15408(Common Criteria)との関係	52
5.2.5 ISO/IEC 27000 シリーズとの関係	53
5.2.6 政府機関の情報セキュリティ対策のための統一基準との関係	54
5.2.7 金融機関等コンピュータシステムの安全対策基準との関係	54
5.2.8 Payment Card Industry Data Security Standard との関係	55
5.3 参考文献	56

1 はじめに

1.1 非機能要求グレード策定の背景とねらい

昨今、情報システムは社会活動、企業活動のために不可欠なものとなっている。図 1.1.1 に情報システムの歴史的な変遷について示す。現在では、IT なしではビジネスは成り立たないものとなっており、また情報システムの利用者も一社内のみならず、社外企業や一般消費者等に広がっている。このような情報システムの社会基盤化に伴い、情報システムのサービスを安定的、確実に提供することが、以前にも増して重要になってきている。また、情報システムの構成要素、すなわち適用される技術・製品は、オープン化、ネットワーク化により、大規模かつ複雑なものとなっている。このため、情報システムの実現のためには、単に業務を IT 化するだけではなく、複雑な構成要素を適切に連携させ、安定的にサービスを提供することが重要となっている。

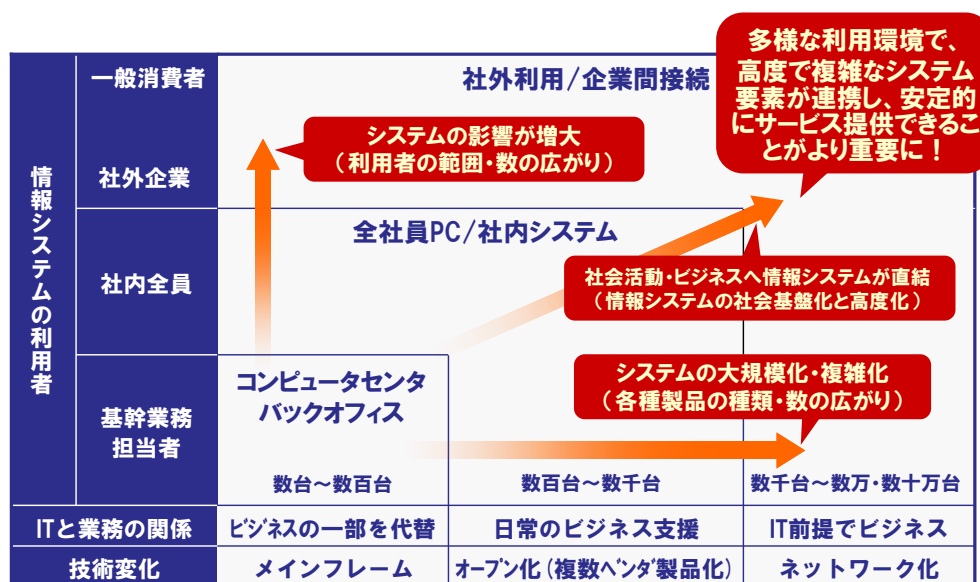


図 1.1.1 情報システムの歴史的な変遷

情報システムは様々な業務機能を実現する業務アプリケーションとそれを支えるためのシステム基盤等で構成される(図 1.1.2)。システム基盤とは、業務アプリケーションに対して共通のサービスを提供する仕掛けのことであり、ハードウェア機器やネットワーク機器、OS やミドルウェア、更にはその制御や運用のアプリケーションなどの組合せで実現される。安定的にサービスを提供するためには、その中でもシステム基盤が重要である。

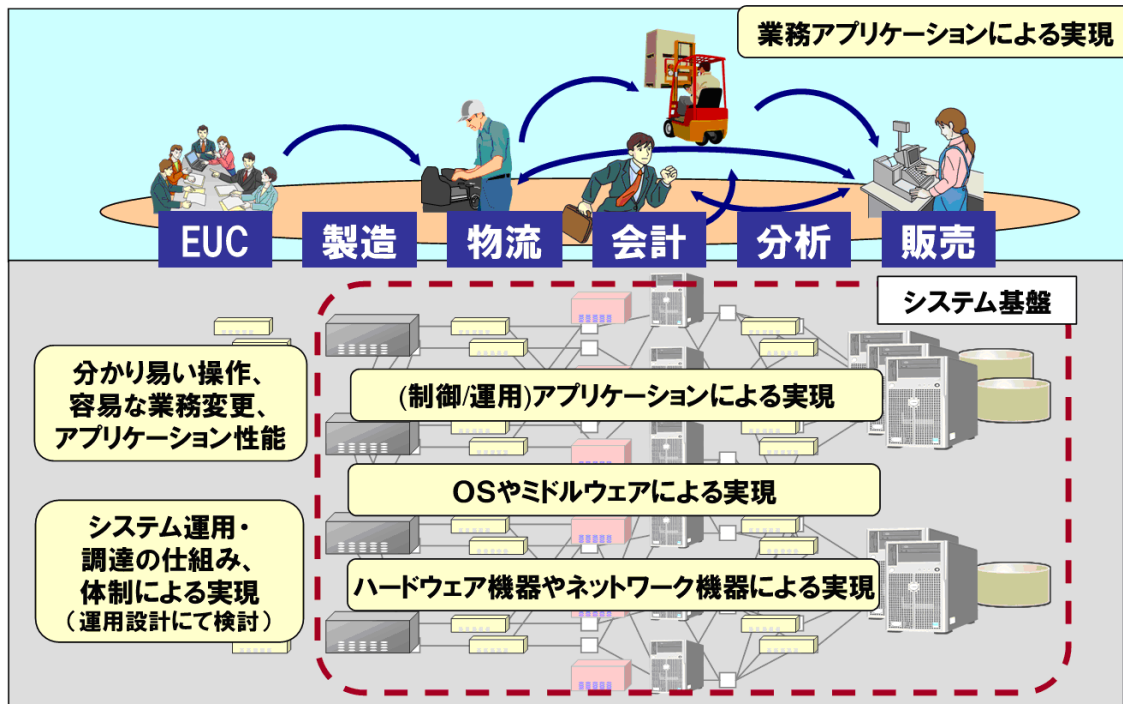


図 1.1.2 システム基盤の位置づけ

情報システムに対する要求には大きく分けて 2 つ存在する。(図 1.1.3)

ひとつは、業務実現に関する要求で、業務の機能そのものを示すことから「機能要求」と呼ばれる。例えば、「営業情報をシステム上で共有し把握したい。」「受発注情報に連動した在庫管理を行いたい。」等の要求である。もうひとつは、「機能要求」以外の要求を意味する「非機能要求」と呼ばれる要求で、例えば、「システムダウン時は 3 時間以内に復旧して欲しい。」等の要求である。システム基盤に関する要求は、主にこの「非機能要求」である。

非機能要求グレードのねらいは、システム基盤に関する非機能要求を明確化し、ユーザ/ベンダ間で認識を共有化することで、適切な情報システムを構築し、安定的なサービスを提供できるようにすることである。

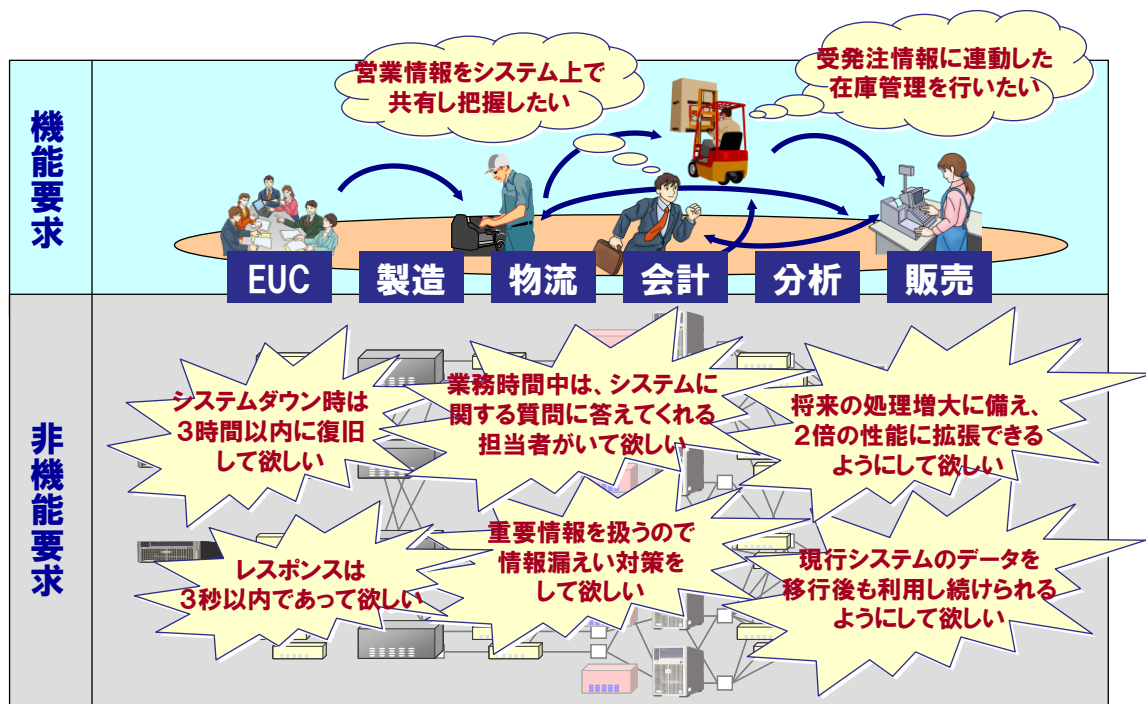


図 1.1.3 機能要求、非機能要求のイメージ

1.2 非機能要求の問題と非機能要求グレードの解決方法

前述したように、情報システムを開発する際には、ユーザ/ベンダ間で非機能要求についての共通認識を持つことが重要である。しかし、実際の情報システム開発の現場においては、ユーザ/ベンダ間で合意すべき非機能要求の漏れや認識違いといったギャップが発生しており、そのギャップの発生が、適切な情報システム開発を阻害している。

図 1.2.1 に、この問題について図示する。

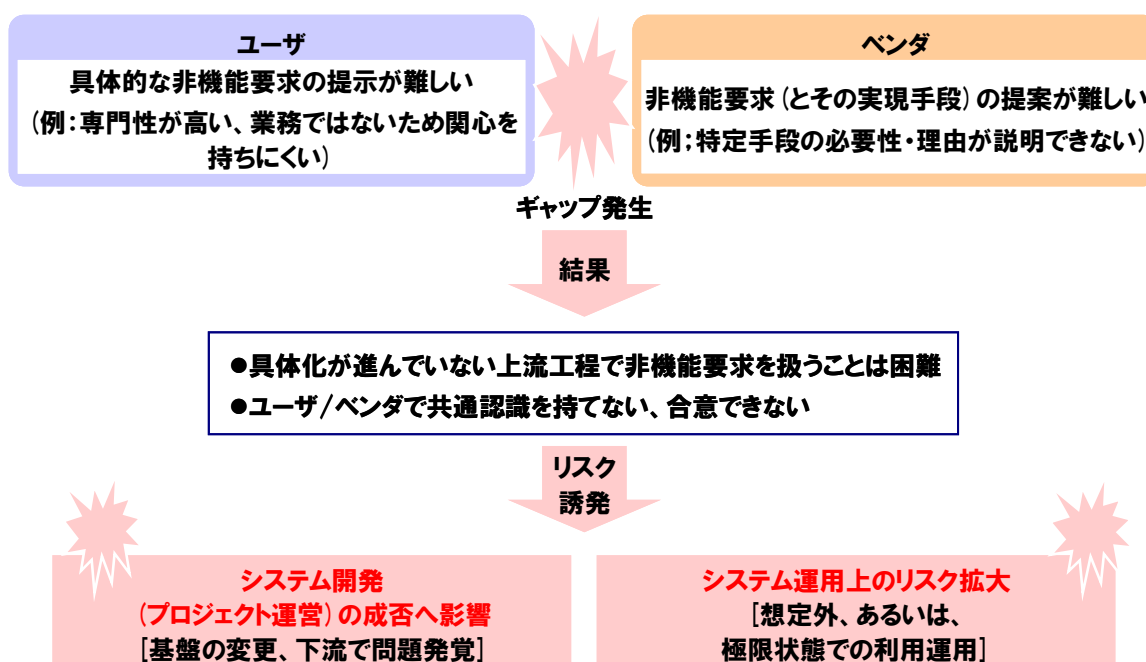


図 1.2.1 非機能要求の問題

ギャップが発生する理由として、非機能要求の検討には専門性が要求されるため、ユーザにとっては開発初期には具体的な非機能要求の提示が難しいことが挙げられる。また、非機能要求は、業務との関係が見えにくい要求であるため、関心を持ちにくいということもある。一方ベンダにとっては、非機能要求とそれを実現する手段について、その必然性や有効性を十分説明できないために、提案が難しいということが挙げられる。

ギャップが発生することにより、非機能要求が明確には定まらないまま開発が進み、下流工程で開発や運用でのトラブルの原因となってしまう。

この問題を非機能要求グレードがどのように解決しようとしているのかを以下に示す。

- ・ ユーザ/ベンダ双方で共通に利用可能なツールとし、かつ一般公開することで、双方の間で合意すべき非機能要求の漏れや認識違いを解消できるようにする。
- ・ 段階的詳細化の手順にあわせたツール構成とし、更に利用方法のガイドを含めることで、ユーザが非機能要求を速やかに提示できるようにする。
- ・ 非機能要求の実現レベルを列挙することで、ベンダが非機能要求の実現手段を具体的に提示できるようにする。

1.3 非機能要求グレードのスコープ

1.3.1 非機能要求の定義とシステム基盤との関係

広義には非機能要求とは、情報システムで実現したい機能要求以外の全ての要求、という文字通りの意味で用いられることがある。そのため、予算などのプロジェクト管理上の要求や情報システムの対象業務を取り巻く法律・ビジネスルールなどを含む場合もあるなど、定義が様々である。

非機能要求グレードでは、非機能要求のうち、主に、システム基盤で実現される要求をスコープとしている。システム基盤に注目している理由としては、これまでの要求定義においては、業務アプリケーションで実現される要求に偏ってしまっていて不足しがちなシステム基盤に対する要求の確認・合意を促すことが必要であると考えているからである。

ただし、非機能要求グレードでは、システム基盤に対する要求を定義する際に重要な要求項目であると考えられるものについては、それ自体は必ずしもシステム基盤で実現されるとは限らないものについても対象に含めている。例として、以下のようなものが挙げられる。

- ・ 運用に関する要求
運用時間など、情報システム全体に関連するが、性能や可用性に関する要求を定義するためにも重要であるもの。
- ・ セキュリティ要求
セキュリティ方針など、他にも影響を与えるが、システム基盤で実現する非機能要求に影響を与える可能性のあるもの。
- ・ 試験に関する要求
試験環境の要否、試験の範囲等、構築するシステム基盤の規模や体制などに影響を与える可能性のあるもの。

また、非機能要求グレードでは、上流工程において、情報システムの設計を開始するまでに、ユーザ/ベンダ間で合意すべき要求項目を対象としている。

以下、本書では特に個別の説明がない限り、非機能要求という用語を、本節で述べた「主にシステム基盤において実現される要求」という意味で用いるものとする。

1.3.2 スcopeとしている項目

非機能要求グレードはシステム基盤に関わる非機能要求をscopeとしている。具体的には、それらの要求を「可用性」、「性能・拡張性」、「運用・保守性」、「移行性」、「セキュリティ」、「システム環境・エコロジー」の6つの大項目に整理している¹。

それぞれの大項目の要求と、その要求に基づいた実現方法の例を表1.3.2.1に示す。

¹ 6大項目に整理した経緯等については、3章FAQのQ1を参照。

表 1.3.2.1 非機能要求グレードの 6 大項目

非機能要求 大項目	説明	要求の例	実現方法の例
可用性	システムサービスを継続的に利用可能とするための要求	<ul style="list-style-type: none"> 運用スケジュール(稼働時間・停止予定など) 障害、災害時における稼働目標 	<ul style="list-style-type: none"> 機器の冗長化やバックアップセンターの設置 復旧・回復方法および体制の確立
性能・ 拡張性	システムの性能、および将来のシステム拡張に関する要求	<ul style="list-style-type: none"> 業務量および今後の増加見積り システム化対象業務の特性(ピーク時、通常時、縮退時など) 	<ul style="list-style-type: none"> 性能目標値を意識したサイジング 将来へ向けた機器・ネットワークなどのサイズと配置 ＝ キャパシティ・プランニング
運用・ 保守性	システムの運用と保守のサービスに関する要求	<ul style="list-style-type: none"> 運用中に求められるシステム稼働レベル 問題発生時の対応レベル 	<ul style="list-style-type: none"> 監視手段およびバックアップ方式の確立 問題発生時の役割分担、体制、訓練、マニュアルの整備
移行性	現行システム資産の移行に関する要求	<ul style="list-style-type: none"> 新システムへの移行期間および移行方法 移行対象資産の種類および移行量 	<ul style="list-style-type: none"> 移行スケジュール立案、移行ツール開発 移行体制の確立、移行リハーサルの実施
セキュリティ	情報システムの安全性の確保に関する要求	<ul style="list-style-type: none"> 利用制限 不正アクセスの防止 	<ul style="list-style-type: none"> アクセス制限、データの秘匿 不正の追跡、監視、検知 運用員などへの情報セキュリティ教育
システム環境・ エコロジー	システムの設置環境やエコロジーに関する要求。	<ul style="list-style-type: none"> 耐震/免震、重量/空間、温度/湿度、騒音など、システム環境に関する事項 CO₂ 排出量や消費エネルギーなど、エコロジーに関する事項 	<ul style="list-style-type: none"> 規格や電気設備に合った機器の選別 環境負荷を低減させる構成

1.3.3 スコープ外の項目について

非機能要求グレードでスコープ外としている項目について、表 1.3.3.1 に示す。

表 1.3.3.1 スコープ外としている項目とその理由

No	スコープ外としている項目	理由	例
1	主に業務アプリケーションを定めるための項目	システム基盤で実現する非機能要求に比べ、ユーザ/ベンダ間で意識されやすく、要求明確化のためのツールも比較的整備されているため。	ユーザビリティ、機能性、移植性など
2	各社個別の製品やソリューションの選択に関する項目	個別製品やソリューションの選択は情報システムの各ユーザに依存するものであり、非機能要求グレードで決定するものではないため。	個別具体的なシステム構成、構成要素、製品など

1.4 非機能要求グレードの概要

本節では非機能要求グレードの基本コンセプトから、非機能要求グレードを構成する3つのツールの利用目的や使い方のポイント、ツール間の関連などについて説明する。

1.4.1 非機能要求グレードの基本コンセプト

(1) レベルによる要求項目の共通認識

非機能要求グレードの基本的な考え方を初めに説明する。

非機能要求グレードでは、ユーザ/ベンダ間でシステム基盤に関わる非機能要求を合意し、認識のズレをなくすことを目的としており、

①非機能要求の項目を、定量的に表現できる指標で表わす

②各項目をコストやアーキテクチャのギャップに応じてレベルを設定する

という方針のもと非機能要求が整理されている。

ユーザ/ベンダ間で非機能要求を合意するとは、上記の要求項目に設定されたレベルを決定し共有することを意味する。要求項目が定量的でなく曖昧な表現で定義された場合（例えば「利用者が満足する性能を満たすこと」など）、要求項目としてお互いに認識することはできたとしても、要求項目の解釈はそれぞれ異なる可能性があり、要求項目をどのように実現するか、あるいは達成できるかを合意することは困難である。要求項目を指標として設定すると同時に、指標値をあらかじめレベル化することで、図1.4.1.1に示すように、実現の難易度やコスト感をユーザ/ベンダ間で認識しやすいものになっている。



図 1.4.1.1 要求項目のレベル化

ただしレベルはあくまでも合意形成の出発点であって、ある程度の幅を持たせている。最終的にはユーザ/ベンダ間で具体的な数値として合意する必要がある。

(2) グレードによる要求項目の選定

非機能要求グレードでは、「グレード」という概念を導入した。

システムは、それぞれその利用目的、規模、そのシステムが社会へ与える影響などが異なっている。こうしたシステムが持つ性質や特徴の多様性があるために、全てのシステムに対

して非機能要求を一意に決めることはできない。これによりシステムを構成する要素となるハードウェア・設備、OS・ミドルウェア、運用管理の仕組み・体制などの組合せと連携により実現水準には差が生じる。開発初期にはその差がユーザからは認識されにくく、ベンダとしても技術を説明するのが難しいという課題がある。しかし、システムの非機能要求を検討し決定する際に、参考となる典型的なモデルを示すことができれば、非機能要求の検討が行いやすくなる。

そこでシステム間の差を「グレード」として段階的に示し、各グレードに要求項目のレベルを設定することで、早期に非機能要求項目をユーザ/ベンダで確認ができる仕組みを提供している。

（３）段階的な要求項目の詳細化

非機能要求グレードは、各ツールにおいて特に利用用途などは限定していないが、非機能要求をユーザ/ベンダ間で段階的に詳細化し合意形成していくことを想定して各ツールを構成している。以下各ツールの概要・利用目的について各ツール間の関係を踏まえて説明する。ツールの詳細説明については２章、利用方法については〔利用編〕を参照されたい。

1.4.2 非機能要求グレードの構成要素・概要

非機能要求グレードを構成する各ツールの概要および非機能要求グレード全体のイメージを図 1.4.2.1 に示す。

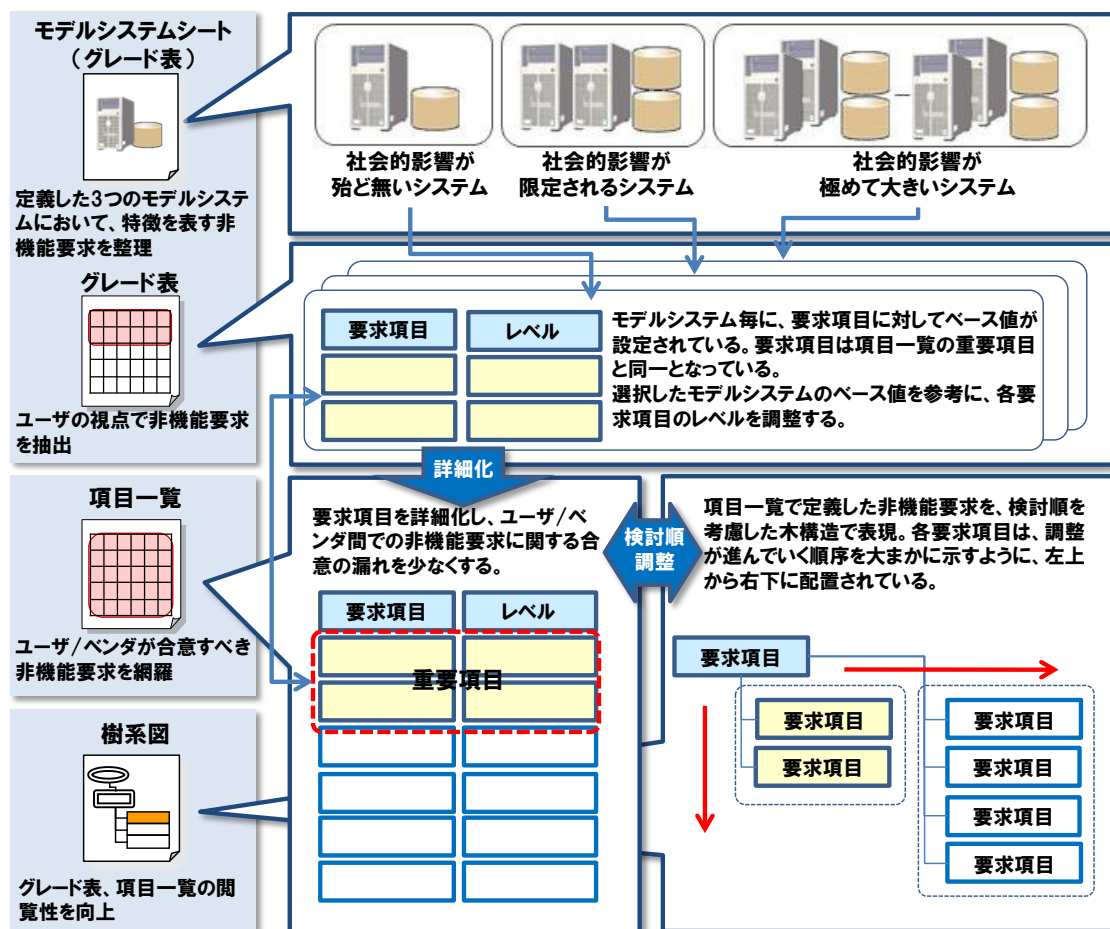


図 1.4.2.1 非機能要求グレードの概要と全体イメージ

(1) グレード表

グレード表とは3つの「グレード」それぞれに非機能要求項目のレベル値を定義したものである。グレード表で対象となる要求項目は、ユーザの視点を踏まえ、品質やコストに与える影響が大きいという観点で選択した項目となっている。そのため、グレード表は項目一覧から重要項目を抽出した表の右側に3つの「グレード」としてレベル値のセットを定義した構成となる。

3つの「グレード」は、グレード表に含まれるモデルシステムシートの中で以下3つのモデルシステムとしてその特性を定義している。

- 社会的影響が殆ど無いシステム
- 社会的影響が限定されるシステム
- 社会的影響が極めて大きいシステム

モデルシステムシートには、ユーザがモデルシステムを選定する際の基準として、それぞれのモデルシステムの特徴を表す非機能要求が定義されている。各モデルシステムの具体

的な説明と設定した非機能要求項目については、2章の非機能要求グレードの詳細で記載している。

1つのモデルシステムには選択レベルと選択時の条件の記述がある。選択レベルにはベース値として各要求項目のレベルの初期値が設定されている。非機能要求を決定していくにあたり、グレード表と合わせて活用することで、モデルシステムで設定されているベース値を参考に決めることができるようになっている。

モデルシステムは、非機能要求項目を段階的に詳細化して合意していく過程をとることで、グレード表を利用した非機能要求の選定を容易にすると共に、まずは重要な非機能要求項目を合意することで、早期にユーザ/ベンダ間での認識のズレを抑えることを目的としている。

(2) 項目一覧

項目一覧は、システム基盤に関わる非機能要求をユーザ/ベンダ間で漏れなく共通に認識できるように項目を体系化した一覧表である。要求項目は表 1.3.2.1 で定義したように6つの大項目に分類されている。項目一覧は図 1.4.2.2 に示すように、各大項目を単位に要求項目を体系的に整理・分類することで網羅性を高めている。

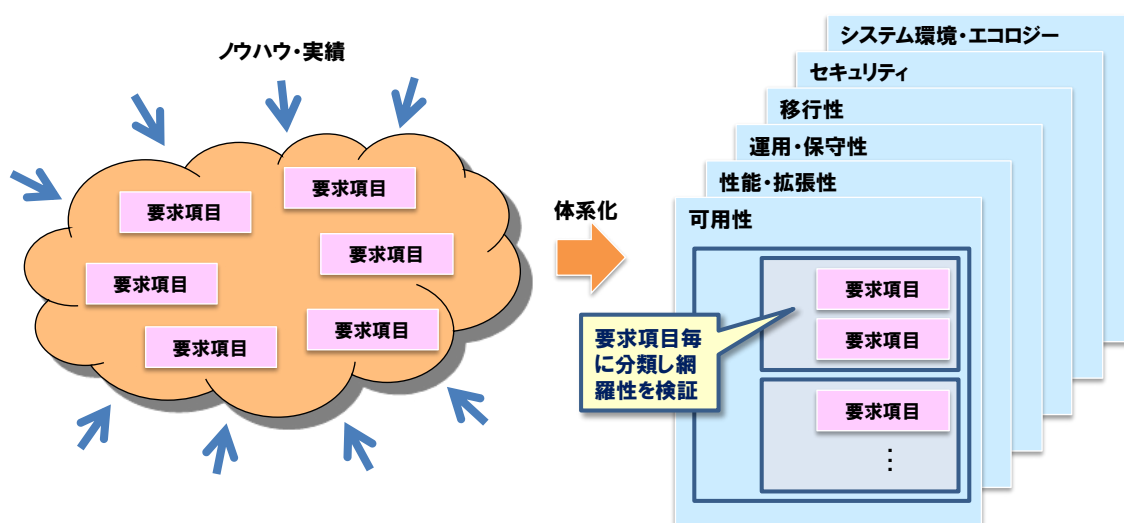


図 1.4.2.2 要求項目の体系化

非機能要求をユーザ/ベンダで合意していく過程はさまざまであるが、最終的に合意すべき非機能要求を一元的に確認できるようにすることが目的である。

項目一覧にはグレード表で定義された非機能要求項目が含まれており、段階的な詳細化の過程において、グレード表で決定した要求項目から更にブレイクダウンして詳細な項目を決定するような利用方法を想定している。

(3) 樹系図

樹系図は、グレード表、項目一覧の閲覧性を向上させ、要求項目の検討順を可視化した図となっている。樹系図はグレード表および項目一覧を利用する際に併せて参照することで、非機能要求項目を段階的に詳細化していく作業を効率化することが目的である。

例えば、グレード表を用いて重要項目のレベルを決定していくようなケースでは、ユーザ/ベンダがお互いに樹系図で非機能要求全体を俯瞰し、次にどの項目を決定するかを確認しながら作業を進めることができる。

2 非機能要求グレードの詳細説明

2.1 非機能要求グレードの詳細説明

非機能要求グレードの各ツールについて、具体例を用いて内容の詳細を解説する。

2.1.1 グレード表

(1) モデルシステムの定義

非機能要求グレードでは、経済産業省の情報システムの信頼性向上に関するガイドライン（以下、信頼性ガイドライン）や IPA の重要インフラ情報システム信頼性研究会報告書を参考にシステムを 3 つに分類し²、それぞれに対してシステムの非機能要求を具体的に定義している。これを以下、モデルシステムと呼ぶ。モデルシステムの定義を図 2.1.1.1 に示す。



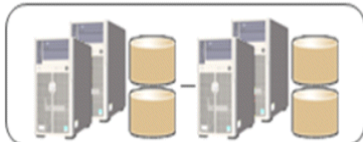
項番	モデルシステム名とそのイメージ	モデルシステムの概要
1	社会的影響が殆ど無いシステム 	企業の特定期間が比較的限られた範囲で利用しているシステムで、機能が低下または利用不可な状態になった場合、利用部門では大きな影響があるが、その他には影響しないもの。 ここでは、ごく小規模のインターネット公開システムを想定している。
2	社会的影響が限定されるシステム 	企業活動の基盤となるシステムで、その機能が低下または利用不可能な状態に陥った場合、当該企業活動に多大の影響を及ぼすと共に取引先や顧客などの外部利用者にも影響を及ぼすもの。 ここでは、企業内のネットワークに限定した基幹システムを想定している。
3	社会的影響が極めて大きいシステム 	国民生活・社会経済活動の基盤となるシステムで、その機能が低下または利用不可能な状態に陥った場合、国民生活・社会経済活動に多大な影響を与えるもの。 ここでは、不特定多数の人が利用するインフラシステムを想定している。

図 2.1.1.1 モデルシステムの定義

(2) モデルシステムの非機能要求項目

各モデルシステムの非機能要求項目を示す際に、名称だけでは非機能要求レベルがわか

² 「重要インフラ情報システム信頼性研究会」のシステムプロファイリングではシステムのカテゴリが 4 つ存在するが、非機能要求グレードにおけるモデルシステムでは、主に経済損失レベルや公共的影響有りといった影響度合を考慮し、「人命への影響、甚大な経済損失が予想されるシステム」を「社会的影響が極めて大きいシステム」の中を含めている。

りにくいため、モデルシステムの特徴を表すような非機能要求項目を抽出し、モデルシステムシートにまとめている。モデルシステムシートを図 2.1.1.2 に示す。



項番	大項目	特徴	社会的影響が殆ど無いシステム	社会的影響が限定されるシステム	社会的影響が極めて大きいシステム
モデルシステムイメージ					
モデルシステムの概要			企業の特定部門が比較的限られた範囲で利用しているシステムで、機能が低下または利用不可能な状態になった場合、利用部門では大きな影響があるが、その他には影響しないもの。 ここでは、ごく小規模のインターネット公開システムを想定している。	企業活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、当該企業活動に多大の影響を及ぼすと共に取引先や顧客等の外部利用者にも影響を及ぼすもの。 ここでは、企業内のネットワークに限定した基幹システムを想定している。	国民生活・社会経済活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、国民生活・社会経済活動に多大な影響を与えるもの。 ここでは、不特定多数の人が利用するインフラシステムを想定している。
1	可用性	稼働率	・1年間で数日程度の停止まで許容できる(稼働率99%)。	・1年間で1時間程度の停止まで許容できる(稼働率99.99%)。	・1年間で数分間程度の停止まで許容できる(稼働率99.999%)。
2		目標復旧水準	・データのリカバリを伴う復旧では、通常のバックアップからの復旧が目標水準となる。	・データのリカバリを伴う復旧では、1営業日以内での復旧が目標水準となる。	・データのリカバリを伴う復旧では、数時間で障害発生時点までの復旧が目標水準となる。
3		大規模災害	・大規模災害時は、システムの再構築による復旧が前提となる。	・大規模災害時は1週間以内での復旧を目指す。	・大規模災害時にはDRサイトでの業務継続性が要求される。 ・バックアップセンターを設置し、大規模災害に備える。
4	性能・拡張性	性能目標	・大まかな性能目標はあるが、他の要求より重視しない。	・性能面でのサービスレベルが規定されている。	・性能面でのサービスレベルが規定されている。
5		拡張性	・拡張性は考慮しない。	・システムの拡張計画が決まっている。	・システムの拡張計画が決まっている。
6		運用・保守性	運用時間	・業務時間内のみのサービス提供で、夜間の運用はない	・常時サービス提供が前提であり、24時間365日の運用を行う。
7		バックアップ	・部門の管理者が必要なデータのみを手動でバックアップする。	・システム全体のバックアップを日次で自動的に取得する。	・運用サイトと同期したバックアップサイト(DRサイト)を構成する。
8		運用監視	・ハードウェアやソフトウェアの各種ログを用いて死活監視を行う	・アプリケーションの各業務機能が正常に稼働しているかどうか監視を行う。	・性能やリソース使用状況まで監視し、障害の予兆検出を行う。
9		マニュアル	・マニュアルは、部門の管理者が独自に作成する。	・サービスデスクを設置してメンテナンス作業も行うため、運用マニュアルとともに保守マニュアルも用意する。	・自センターの運用ルールに合わせて運用マニュアルをカスタマイズする。
10		メンテナンス	・必要に応じて随時メンテナンス作業を行っても良い。	・日中の運用に影響しなければ、システムを停止してメンテナンス作業を行ってもよい。	・メンテナンス作業はすべてオンライン状態で実施する。
11	移行性	移行方式の規定	・移行方式についての規定は特に無い(ベンダ側からの提案により合意する)。	・業務の効率化を目指し、積極的に統合化やアプリケーションの変更を行う。 ・システムの切替は一斉に行う。	・移行リスクを少なくするため、段階的に移行する。
12		移行スケジュール	・移行の日程は十分に確保される。	・移行のためのシステム停止は可能である。	・移行のための停止時間を最小限にする。
13		設備・データ	・設備やデータは新規構築とする。	・設備やデータの変更がある。	・設備やデータの移行があるが、データベース構築はデータの継続性や他システムとの親和性を担保するため、積極的には変更しない。
14	セキュリティ	重要資産の公開範囲	・セキュリティ対策を施すべき重要な資産を保有していない。 (重要資産とは個人情報、センシティブ情報、資金性の高い情報などのように特に高いセキュリティが必要な情報資産のこと)	・セキュリティ対策を施すべき重要な資産を保有しているが、特定の相手とのみ繋がっている。	・セキュリティ対策を施すべき重要な資産を保有しており、不特定多数の利用者にサービスを提供される。
15	システム環境・エコロジー	制限	・法律や条例などの制限はない。	・法律や条例などの制限が多少ある。	・法律や条例などの条件が有り。
16		耐震	・耐震は最低限のレベルで必要である。	・耐震は通常レベルの対策が必要である。	・耐震は高いレベルで必要である。

図 2.1.1.2 モデルシステムシート

また、モデルシステムの特徴を大項目毎にまとめた表を表 2.1.1.1 に示す。

表 2.1.1.1 モデルシステムの特徴

大項目	特徴的な非機能要求
可用性	稼働率、目標復旧水準、大規模災害
性能・拡張性	性能目標、拡張性
運用・保守性	運用時間、バックアップ、運用監視、マニュアル、メンテナンス
移行性	移行方式の規定、移行スケジュール、設備・データ
セキュリティ	重要資産の公開範囲
システム環境・エコロジー	制限、耐震

モデルシステムシートは図 2.1.1.2 に示すものをグレード表に含めて提供し、段階的詳細化の1段階目に活用してもらうことを想定している。段階的詳細化については[利用編] 1.1 節 (1) を参照頂きたい。

(3) グレード表の例

グレード表は項目一覧から重要項目を抽出した表の右側に 3 つのモデルシステムに対するグレードを定義した形式となっている。グレード表の例を図 2.1.1.3 および図 2.1.1.4 に示す。

本項ではグレード定義を拡大した図 2.1.1.4 について説明する。

グレード表のモデルシステムに関する記述より左側の列は、重要項目列の有無を除いて、項目一覧と同様である。項目一覧の各項目についての説明は 2.1.2 項で行う。

項目	大項目	中項目	小項目	小項目説明	マトリクス (階層)	レベル					運用への 影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム	
						0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル
A.1.1.1	可用性	可用性	可用性	システムの稼働時間や停止時間に関する情報	○	運用時間(通常)	規定無し	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	【重要項目】 C.1.1.1. 運用時間は、システムの可用性の実現レベルを確保する項目であるとともに、運用・保守性に関する観点から運用コストを抑制する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【リスク】 運用時間は、オンライン/パッチを各システムが稼働している時間を指す。 【レベル】 この項目は各レベルの一例を示したもので、レベル選択の条件とはしていない。「規定無し」は、規定のサービス時間が存在しないことを指し、基本的にシステムは停止していない。必要に応じてユーザーがシステムを稼働する必要がある場合(例: 稼働中にシステムが停止した場合、稼働・稼働中システム等)「夜間のみ」が夜間のみは、一般的な業務稼働を想定したもので、業務稼働する時間帯に稼働するシステムにおいては、稼働中や稼働中の稼働を必要とする。「停止あり」とは、システム停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。「24時間稼働」は、オンライン/パッチが稼働している時間帯にシステム稼働を必要とする。システムを停止することができないようなケースも含まれる。	2 夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	4 夜間のみ停止(9時~21時)	5 24時間無停止	
A.1.1.2	可用性	可用性	可用性	システムの稼働時間や停止時間に関する情報	○	運用時間(特異日)	規定無し	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	夜間のみ停止(9時~21時)	【重要項目】 C.1.1.2. 運用時間は、システムの可用性の実現レベルを確保する項目であるとともに、運用・保守性に関する観点から運用コストを抑制する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【リスク】 運用時間は、オンライン/パッチを各システムが稼働している時間を指す。 【レベル】 この項目は各レベルの一例を示したもので、レベル選択の条件とはしていない。「規定無し」は、規定のサービス時間が存在しないことを指し、基本的にシステムは停止していない。必要に応じてユーザーがシステムを稼働する必要がある場合(例: 稼働中にシステムが停止した場合、稼働・稼働中システム等)「夜間のみ」が夜間のみは、一般的な業務稼働を想定したもので、業務稼働する時間帯に稼働するシステムにおいては、稼働中や稼働中の稼働を必要とする。「停止あり」とは、システム停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。「24時間稼働」は、オンライン/パッチが稼働している時間帯にシステム稼働を必要とする。システムを停止することができないようなケースも含まれる。	3 規定無し	週末と異なる運用時間となる特定日は存在しない。	2 夜間のみ停止(9時~21時)	5 24時間無停止	
A.1.1.3	可用性	可用性	可用性	システムの稼働時間や停止時間に関する情報	○	計画停止の有無	計画停止無し	計画停止あり(運用スケジュールの変更不可)	計画停止あり(運用スケジュールの変更不可)	計画停止あり(運用スケジュールの変更不可)	計画停止あり(運用スケジュールの変更不可)	計画停止あり(運用スケジュールの変更不可)	【重要項目】 C.1.1.3. 計画停止の有無は、システムの可用性の実現レベルを確保する項目であるとともに、運用・保守性に関する観点から運用コストを抑制する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【リスク】 計画停止は、オンライン/パッチを各システムが稼働している時間を指す。 【レベル】 この項目は各レベルの一例を示したもので、レベル選択の条件とはしていない。「規定無し」は、規定のサービス時間が存在しないことを指し、基本的にシステムは停止していない。必要に応じてユーザーがシステムを稼働する必要がある場合(例: 稼働中にシステムが停止した場合、稼働・稼働中システム等)「夜間のみ」が夜間のみは、一般的な業務稼働を想定したもので、業務稼働する時間帯に稼働するシステムにおいては、稼働中や稼働中の稼働を必要とする。「停止あり」とは、システム停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。「24時間稼働」は、オンライン/パッチが稼働している時間帯にシステム稼働を必要とする。システムを停止することができないようなケースも含まれる。	3 計画停止あり(運用スケジュールの変更不可)	事前の合意があれば、停止は可能。	2 計画停止あり(運用スケジュールの変更不可)	5 24時間無停止	



図 2.1.1.3 グレード表の例 (全体)

社会的影響が殆ど無いシステム			社会的影響が限定されるシステム			社会的影響が極めて大きいシステム		
選択レベル	選択時の条件		選択レベル	選択時の条件		選択レベル	選択時の条件	
2	夜間のみ停止(9時~21時)	夜間を実施する業務はなく、システムを停止可能。 [-] 運用時間をもっと限って業務を稼働させる場合 [+] 24時間無停止やリポート処理等の短時間の停止のみを考える場合	4	若干の停止有り(9時~翌朝8時55分)	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [-] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [-] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
0	規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日にバックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ停止(9時~21時)	週末はバックアップ運用のための、夜間は停止する。 [-] 週末運用するバックアップやパッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日でも運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [-] 定期的に運用を停止する日が存在する場合
0	計画停止有り(運用スケジュールの変更不可)	事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止有り(運用スケジュールの変更不可)	24時間無停止での運用は必要ない。停止可能な時間帯が存在し、計画的な停止は可能。 [-] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止無し	システムを停止できる時間帯が存在しない。 [-] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合

図 2.1.1.4 グレード表の例 (グレード定義を拡大)

(4) グレード定義列の説明

各列の説明は以下のとおり。

(a) 選択レベル

非機能要求毎に定義したレベルの中から該当するモデルシステムを想定して選択したレベル。0～5 で示されるレベル値と対応するレベルの説明で構成される。ここで選択されているレベル値をベース値と呼ぶ。

ベース値は原則として左から右にレベルが高くなるが、一部のメトリクスではレベルが逆転したり、同じレベルとなっている場合がある。

レベルが逆転しているメトリクスは、モデルシステム毎の特徴を定義するときに、モデルシステムの名前に合わせた特徴を定義したためである。例えば、「D.4.1.2 移行データ形式」は、移行性の特徴である設備・データに対応し、社会的影響が極めて大きいシステムの場合はデータの継続性を重視して積極的には変更しないと定義し、社会的影響が限定されるシステムではデータの変更があると定義しているため、社会的影響が限定されるシステムの選択レベルが一番大きくなっている。

一方、全て同じレベルになっているメトリクスは、システムのベース値としてはどんなシステムでも同じになるが、決まっていない場合のリスクが大きいものをメトリクスとして定義しているためである。例えば、「B.1.1.3 データ量」は要件定義時には決まっているべきであるため、全てレベル 0 を定義している。

(b) 選択時の条件

ベース値を選択した時の条件。ベース値だけでは実現するシステムの非機能要求を適切に提示できない場合を想定し、ベース値を変更する条件を[－][＋]で示した。

対象システムの非機能要求レベルを下げたい場合は[－]に書かれている条件を確認し、逆に非機能要求レベルを上げたい場合は[＋]に書かれている条件を確認の上レベル調整を行う。

(5) 重要項目選択の経緯

項目一覧は非機能要求項目をリストアップしたツールで 238 メトリクスがある。これらのメトリクスには決定順序が異なるものやシステム基盤のコストに対する影響度合が異なるものなどがあり、何らかのグルーピングが必要である。更に、項目数が多すぎて検討に時間がかかるといった点も考慮し、メトリクスを選択している。これを重要項目と定義する。重要項目の選択にあたってはコストや品質に影響を与える度合が大きいメトリクスをユーザ視点とベンダ視点の両面から評価し選択している。³

(6) グレード表の活用イメージと効果

ユーザが提示した要求レベルに対するベンダの見積もり回答が予算に合わなかった場合

³ 評価の経緯は非機能要求グレード「ユーザビュー検討委員会」報告書を参照。

に、選択レベルを変更して再見積りを要求するというサイクルが想定できる。このような場合にコスト超過を理由に当初の非機能要求を変更するとシステム基盤の品質がどのように変わるかが視覚的に確認しやすくなる。

(7) グレード表のテーラリング

グレード表では 3 つのモデルシステムを用いてベース値を定義しているが、ユーザ/ベンダそれぞれがグレード表を活用していくために、自組織固有のモデルシステムをグレード表に追加することが可能である。例えば、『XX社の社内システムのためのモデルシステム』や『学校図書館管理システムのためのモデルシステム』などである。実際に稼働しているシステムを用いたグレード表を定義することで、多くの類似するシステムの非機能要求をより高い精度で策定できるようになる。

2.1.2 項目一覧

(1) 項目一覧の例

項目一覧は、システムの開発や運用を行う上で、システム基盤に関わる判断をするために、ベンダとユーザが確認する非機能要求項目のリストであり、項番、大項目、中項目、小項目、小項目説明、重複項目、重要項目、メトリクス（指標）、レベル、運用コストへの影響、備考から構成されている。項目一覧の例を図 2.1.2.1 に示す。

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス (指標)	レベル						運用コストへの影響	備考
								0	1	2	3	4	5		
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。			運用時間 (通常)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の 停止有り (9時～翌朝8時)	若干の停止 有り (9時～翌朝8時55分)	24時間無 停止		【重複項目】 C.1.1.1. 運用時間は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 運用時間は、オンライン/バッチを含みシステムが稼働している時間帯を指す。 【レベル】 0内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。「規定なし」は、固定のサービス時間が存在しないことを示し、基本的にシステムは停止して、必要に応じてユーザがシステムを起動するようなケースを想定している(例:障害発生に備えた予備システム、開発・検証用システム等)。「定時内」や「夜間のみ」は、一般的な業務形態を想定したもので、業務が稼働する時間帯が異なるシステムにおいては、時間帯をスライヤさせるなどの読替えが必要である。「停止あり」は、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。「24時間無停止」は、オンライン業務が稼働していない時間にバッチを稼働させる必要があり、システムを停止することができないようなケースも含まれる。
A.1.1.2							運用時間 (特定日)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の 停止有り (9時～翌朝8時)	若干の停止 有り (9時～翌朝8時55分)	24時間無 停止		【重複項目】 C.1.1.2. 運用時間は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 特定日は、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある(例:「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリポートをするためその日はレベル3」など)。 また、「ユーザの休日」だけでなく、「ベンダの休日」についても特定日として認識し、運用保守体制等を整合すること。
A.1.1.3							計画停止の有無	計画停止有り(運用スケジュールの変更可)	計画停止有り(運用スケジュールの変更不可)	計画停止無し				○	【重複項目】 C.2.1.1. 計画停止の有無は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【運用コストへの影響】 計画停止が「有り」の場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかかる。

図 2.1.2.1 項目一覧の例

(2) 項目一覧構成列の説明

以下、各項目について左側から順に説明する。

(a) 項番

大項目、中項目、小項目、メトリクスでの連番を示す番号。大項目のみを英字 (A～F) で表し、中項目からメトリクスまでをピリオドで区切った連番で示す。

(b) 大項目

非機能要求を体系的に整理した時の最も広い分類。

(c) 中項目

小項目を、同一単位で検討すべき単位でまとめた分類。

(d) 小項目

ユーザとベンダの間で合意される非機能要求を示す項目。

(e) 小項目説明

小項目の内容や考え方を示す説明。

(f) 重複項目

大項目間で重複する項目。非機能要求グレードでは、大項目毎に検討対象者や検討順が異なることを想定し、それぞれの大項目の観点で項目を選択しているため、重複が存在する。

どちらか一方の大項目に集約してしまうことによる検討漏れを防ぐと共に、全体をまとめて検討する場合には、本列を見て重複項目かどうか判断できるため、検討の重複を防ぐことが可能である。

(g) 重要項目

非機能要求を検討する上で品質やコストに大きな影響を与える項目。重要項目として選択された項目はグレード表を構成する項目として使用している。

(h) メトリクス (指標)

小項目を定量的に表現するための指標。システムの構成によっては、1つのメトリクスで複数のレベル合意が必要な場合がある。

例えば、「B.2.1.1 通常時レスポンス順守率」では、システム全体での順守率を決めるのではなくサービスの重要度や使用頻度に応じてサービス毎に順守率を定めることが多い。

(i) レベル

メトリクスを評価軸として、項目が通常取りうる値をレベル 0 からレベル 5 の 6 段階に整理した項目。レベルの差はアーキテクチャにギャップがあり、レベルが大きいほど実現の難易度が高く、一般的に開発コストが高くなることを表す。

開発コストとは、要件定義後からシステムが出来上がってサービスインするまでの期間にかかるコストのことを言い、ハードウェア、OS やミドルウェア、システム設計、導入時作業などシステム基盤に係わる全てのコストが含まれる。

また、レベル値はメトリクス毎に独立して設定している。つまり全てのメトリクスで同じレベルを選択しても特別な意味は持たない。例えば、レベル 3 は標準的なシ

システム、レベル 4 は基幹システム、レベル 5 は高度な社会基盤システムとはならない。

レベルの段階が 6 つに満たない場合には左詰めで記述している。

(j) 運用コストへの影響

開発コストをかけることで運用コストを下げられる可能性のあるメトリクス。

運用コストとは、サービスイン時点からシステムの保守や管理を行うためのコストのことを言う。運用担当者の人件費、ハードやミドルの保守費、消耗品費などが該当する。運用コストへの影響欄に○がついているメトリクスは、開発コストと運用コストがトレードオフの関係である可能性があることを示している。例えば、「C.1.2.4 バックアップ自動化の範囲」のメトリクスを参照すると、運用コストへの影響欄に○がついている。レベル 0 の「全ステップを手動で行う」というのに比べ、レベル 2 の「全て自動で行う」では自動化機能を組み込むために開発コストは増大するが、運用時には少ない要員でまかなえるため運用コストを削減できる。

レベルの選択を行うときは、運用コストへの影響欄に注意し、○が付いている場合には構築後の運用コストやシステムのライフサイクルにも配慮する必要がある。

(k) 備考

メトリクス毎の補足説明。項目一覧の構成で表現しきれない点を記述している。特に、以下に示す内容については重点的に記述している。

- ・複数の大項目に同じ項目がある場合（重複項目）の考え方
- ・運用コストへの影響の具体的内容説明

また、備考列の内容が、どの列に対するものかを明記するため、以下の表記方法で記述している。

- ・【メトリクス】、【レベル】などのように列名を【 】で括って表示する。
- ・特定のレベルへのコメントの場合は【レベル 0】のような表現とする。

(3) 非機能要求グレードにおけるレベルについて

グレード表および項目一覧に記載されているレベルは原則的に 0 から順に数値が大きくなるほど開発コストが増えるように設定されている。

一部のメトリクスについてはレベルが 0 および 1 の二値で表現されているものがある。原則として、二値のメトリクスもレベルの高い方が、開発コストが大きくなっている。しかし、二値であるためにコスト感が実感しにくいメトリクスもある。この場合は、以下の 3 つの観点から評価してレベルを決定している。

- ① 法的な制限や対策実施の有無などを表現する場合の「単純二値」
- ② 具体的な値が定まっていない場合などにそのリスクを想定した「リスク順」
- ③ 実現の難しさを配慮した「難易度順」

いずれも直接的には開発コストをイメージしにくいかもしれないが、法や条例、業界の取

り決めなどといった外的な制限があれば、開発コストは増加しやすく、また具体的な要求が提示されていなければシステムに対するリスクは高く、開発コスト増大の可能性が高くなる。また要求が複雑で難易度が高くなれば、設計の難易度も高くなり、コストが増大しやすくなることが言える。

レベルはユーザとベンダが非機能要求に対してより正確な合意ができるように代表値が設定されているが、項目によってはレベルの選択だけでなく、具体的な値まで決定し合意することが望ましい。例えば「A.1.1.1 運用時間（通常）」のレベル1にある「定時内」の定義はユーザやシステム毎に異なり、レベルにある「9 時～17 時」と必ずしも一致しない。また、「A.1.2.2 サービス切り替え時間」のレベル1は24 時間未満、レベル2は2 時間未満となっているが、この間の時間を設定したい場合も考えられる。

2.1.3 樹系図

(1) 樹系図の定義

樹系図は、グレード表や項目一覧の閲覧性を高めるために図示したものである。

樹系図上の項目は、ユーザ/ベンダ間で調整が進んでいく順序を大まかに示すように、左上から右下に配置されている。厳密な定義はしていないが、左から右への流れは大まかに中項目の検討順を示し、上から下の流れは各小項目単位の検討順を示している。

メトリクスに項番を付加することで他のツールと併用しやすくし、重要項目はメトリクスに網掛けをすることで他のメトリクスとの違いを示している。

樹系図の例を図 2.1.3.1 に示す。

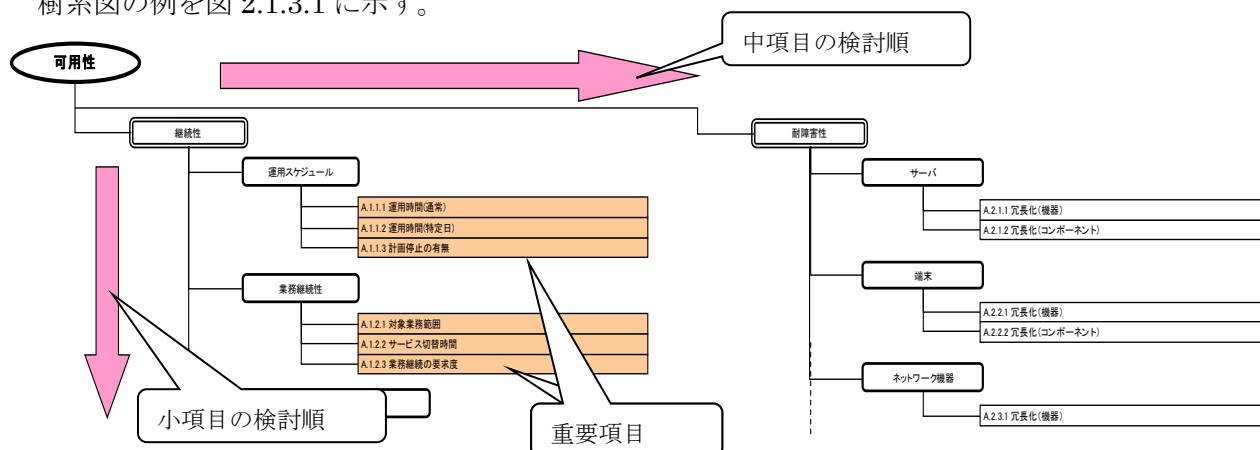


図 2.1.3.1 樹系図の例

(2) 樹系図の利用方法

非機能要求の検討をする際に全体像を確認するために利用する。

具体的には、各大項目のメトリクスについて検討順や重要項目が1枚で閲覧できることを活かして、非機能要求検討時の進め方の確認や、検討が進んだ範囲を確認することなどに活用できる。

2.2 各大項目の概要と留意事項

非機能要求グレードの各大項目について、概要と留意事項に分けて以下に示す。

2.2.1 可用性

(1) 概要

可用性は、システムを継続的に利用可能とするための要求である。システムは何事も問題なくサービスが継続できることが望ましい。しかしシステムは、ハードウェアの障害や OS を含むソフトウェア要因による障害、災害など、様々な要因により、予期せぬサービス停止が発生する。いかにサービスを停止させないようにするか、あるいはサービス停止が発生したとしても影響範囲を極小化し、システムの稼働品質を保証するかが可用性として検討すべきこととなる。

可用性は、「継続性」、「耐障害性」、「災害対策」、「回復性」の4つの中項目から構成される。

(2) 留意事項

「継続性」は可用性を検討する上での基本要素であり、小項目「運用スケジュール」、「業務継続性」、「目標復旧水準」、「稼働率」の4つを定義している。これら小項目に含まれるメトリクスは全て重要項目となっている。可用性での要求を明確にするには、どのような状態をシステムが稼働しているとするかの定義や、障害発生時の復旧目標を明らかにする必要がある。前者は小項目「運用スケジュール」や、小項目「業務継続性」のメトリクス「対象業務範囲」などで、後者は小項目「目標復旧水準」や、小項目「業務継続性」のメトリクス「サービス切替時間」などで確認する。最終的にこれらの定義を用いて稼働率が求められる。システムが稼働しているという定義が異なると、求める稼働率も変わってくるため、これらの定義を明確にしておくことが重要である。稼働率は実際にはシステムが稼働した実績などから計算されるが、可用性を要求する際の目安ともなるため、「継続性」の重要な項目として小項目「稼働率」を位置付けている。メトリクス「稼働率」では、各レベル値は数値として表現しているが、業務をどれだけ継続させたいかという要求に置き換えて検討する。グレード表および項目一覧の「稼働率」の備考欄にその目安を記載しているので参考にしたい。

「耐障害性」は障害に対する耐性への要求を、システムを構成する要素の単位で分類している。「耐障害性」の各項目は「継続性」で確認した内容に応じて検討することが必要である。「継続性」の要求を考慮せずに、「耐障害性」だけに着目して検討してしまうと、ユーザが期待するシステムの信頼性とベンダが提案する対策にズレが生じることがあるので注意が必要である。例えば、「継続性」の小項目「目標復旧水準(業務停止時)」のメトリクス「RLO(目標復旧レベル)」で、要求されるレベルが特定業務のみであったとする。このような場合、サーバの冗長化は、重要な業務が稼働する特定のサーバを冗長化することが望ましい。

しかし小項目「業務継続性」のメトリクス「サービス切替時間」として 60 秒未満が要求されていた場合、「耐障害性」の観点から信頼性を高めようと、全てのサーバを冗長化する選択をしてしまうと、「継続性」での要求に比べて過剰なシステム構成となる。このような要求と対策の認識のズレが発生しないよう、それぞれの項目について要求レベルを確認しながらシステム構成について合意をとる必要がある。

また「耐障害性」では冗長化の項目を機器レベルと、機器内のコンポーネントレベルで分けている。これは、可用性の要求が低いシステムでは単一サーバ構成での耐障害性の要求が見落とされがちであり、このような見落としを防ぐことを目的としている。例えば、サーバを冗長化しない単一サーバ構成とし、ハードウェア故障などが発生した場合、復旧に時間がかかったとしてもサービスは継続して再開できるようにしておきたい。そのため、サーバが停止してもデータだけは喪失しないように、データを格納しているディスクを冗長構成にしておくなど最低限の対策は実施しておくべきである。機器の冗長化という一括りの項目で、部分的対応が見過ごされないよう配慮が必要である。

「災害対策」は、耐障害性に関する要求のうち、特に大規模災害に対する要求項目である。この項目はシステムを構築する上でサーバやストレージなどの構成に影響を与える。初期は遠隔地へのバックアップが不要でも、将来的に必要となる場合には、それが実現できる装置を最初から選択しておくことが必要である。実現できない装置を選択してしまうと、最悪の場合はその装置の置き換えで二重投資などが発生する。業務の継続性を検討する上で、災害対策を考慮するか否かは、コスト的に大きな比重を占めることから1つの大きなテーマとなっている。

「回復性」は、障害が発生した際に、システムを回復し、影響するデータを復旧できる能力とそれに必要な労力に関する要求項目であり、小項目「復旧作業」、「可用性確認」の2つを定義している。「継続性」の検討で目標復旧水準は明確にしているので、この項目ではその復旧水準を実施するにあたっての必要な仕組みと労力を明確にすることが目的である。

「復旧作業」はバックアップからのリカバリ作業をどこまで自動化するかという項目と、業務が停止している間に代替業務を用意できるかという項目で構成され、どちらも運用・保守性と重複項目となっている。

「可用性確認」は可用性として要求された項目がシステムとして実現できているかの確認範囲を明確にする項目である。実際に確認を行う場合は擬似的に障害を発生させて個々の動作が要求通りかを確認する必要があるため、場合によっては確認が困難なケースも存在する。またシステムの規模によっては確認作業にかかるコストも膨大になる。そのため、早期にどこまでを確認の範囲とするかを調整しておくことが重要となる。

2.2.2 性能・拡張性

(1) 概要

性能・拡張性は、システムの性能と将来のシステム拡張に関する要求である。サービスを提供する際にリソースが効率よく使えるかを示すものが性能であり、主にレスポンスやスループットで要求を表現する。レスポンスはサービスを受ける側が要求を出してからサービスが受けられるまでの時間、スループットは単位時間あたりどの程度のサービスを受けられるかという量を示している。要求が不明確な場合、遅くて実用に耐えないシステムになったり、必要以上に高性能なシステム基盤が導入されてしまうことになるため重要である。システムのアーキテクチャは様々であるため、レスポンスやスループットの目標を定める際には用語の定義を明確にする必要がある。

システムは一度構築すると長い期間使われることが多く、この間に利用者数や格納するデータ量などが増えることでシステムのリソースが不足し、システムが本来の役割を果たせなくなることがある。この対策として拡張性を考慮する必要がある。代表的な拡張性の例には、個々のリソースをより大きなものに入れ替えること（スケールアップ）、サーバや機器を追加すること（スケールアウト）がある。要件定義時に見込んでおくことで、機器増設の計画が立てやすく、あらかじめ余裕のある機器構成とすることで、増設時のコストを低くすることも可能である。

性能・拡張性は、前提条件である「業務処理量」、性能に関する要求である「性能目標値」、拡張性に関する要求である「リソース拡張性」、補助的な要求項目である「性能品質保証」の4つの中項目から構成される。

(2) 留意事項

性能・拡張性に関する非機能要求を合意する場合、「業務処理量」をはじめに決めることが一般的である。業務というと機能要求のように思われるかもしれないが、システム基盤の非機能要求を決める上で重要であり、特に性能・拡張性では必須の確認項目である。対象システムがどのようなシステムで、その上で動くおおまかな業務量として小項目「通常時の業務量」を、システムの利用期間における業務量の増加度合として小項目「業務量増大度」を決めておく必要がある。「通常時の業務量」や「業務量増大度」がわからない場合でも、わからない理由や決定可能時期などについて明確にし、ある程度余裕を持った値を仮決めしておくことが重要である。ここではメトリクス「ユーザ数」、「同時アクセス数」、「データ量」、「オンラインリクエスト件数」、「バッチ処理件数」、「業務機能数」の6つを挙げたが、システムの特性に応じて選択・追加を行うことで性能・拡張性に対する要求を明確にすることが出来る。

「性能目標値」は前提となる業務処理量を考慮し、システムの処理形態やピーク特性や縮退時を考慮した性能目標の設定が必要である。

バッチやオンラインのような処理形態の違いによって考慮すべきポイントも異なる。小項目「バッチレスポンス」を例にとると、バッチでは処理時間が長時間かかることをふまえ、レスポンス目標値としては処理の順守度合いで示し、決められた時間内で処理ができるか、障害発生時に再実行の余裕があるのかなどを決める。

一方で、小項目「オンラインレスポンス」ではシステム全体で1つの値を設定するのではなく、参照系と更新系の違いやシステムの重要性に基づいて処理毎に順守率で示し、該当処理の何%が決められた時間内となっているかを定めることでシステムに適切な性能目標値を定めることが出来る。目標設定を誤るとシステムの処理能力が不足し十分なサービスが提供できなくなったり、逆に必要以上に高コストなシステムを構築してしまうことになる。

ピーク時の性能目標を決めるためには、処理毎に、通常時と比べた処理量がどの程度増えるのか、ピークとなる頻度や時間帯などが予見できるのかなどを考慮する。縮退時の性能目標を決めるためには、処理毎に、優先度や重要度を確認しておきたい。

「リソース拡張性」では、システム稼働時にリソースがどれだけ使われているか、別の視点で考えるとどれだけ空きがあるかを決めておきたい。空きがあるかを示すには、サービス開始時点での利用率や、物理的にリソースが増設可能かどうかについて小項目「CPU 拡張性」、「メモリ拡張性」、「ディスク拡張性」で確認する。プリンタやミドルウェアなど他のリソースがあれば必要に応じて追加することを推奨する。システムの成長に合わせて計画的にスケールアップやスケールアウトができるような構成にしておくことが必要である。

「性能品質保証」では性能品質を高めるための仕組みを検討する。

小項目「帯域保証機能の有無」ではネットワークの帯域保証がされているか、されている場合はどのレベルでの保証なのかを確認しておきたい。画像、動画などシステムで扱うデータ量が増えてきているため、CPU やメモリ以上にネットワーク性能がレスポンスに影響するためである。

小項目「HW リソース専有の有無」では、CPU やメモリのリソースを専有するのか、他サーバと共有するのかを決める。

小項目「性能テスト」では、「性能目標値」の実現度合いを評価するためのテストをどの程度行うかを定める。システムによっては、システム構築時の条件と運用が始まってからの条件が変わる場合もあるため、稼働後に定期的に確認することが必要な場合がある。

2.2.3 運用・保守性

(1) 概要

運用・保守性は、システムの運用と保守のサービスに関する要求である。運用や保守に関する要求項目は、システムの運用方法や管理者の作業手順を決定するものであり、導入する機器やソフトウェアの選定にも大きく影響する。システムの開発には関係しないとして検討を後回しにしていると、後になって「想定していた運用スケジュールが組めない」とか、「必要なバックアップがとられておらず、障害からの復旧ができない」といったトラブルを引き起こす原因となる。そういったトラブルを防止するため、要件定義の段階で十分に検討しておく必要がある。

運用・保守性は、正常時、メンテナンス作業時、障害発生時のそれぞれの運用パターンに対する要求を検討する「通常運用」、「保守運用」、「障害時運用」と、それらシステム運用を実現するためにどのような環境や体制を整えるかを検討する「運用環境」、「サポート体制」、「その他の運用管理方針」の6つの中項目から構成される。

(2) 留意事項

「通常運用」には、システムを利用する時間に関する要求項目をまとめた小項目「運用時間」の他に、システム基盤にて実現され得る機能として小項目「バックアップ」、「運用監視」、「時刻同期」の3つを定義している。小項目「運用時間」は、運用・保守性の観点と共に可用性の観点でも検討する必要があるため、重複項目になっている。また、小項目「運用時間」には、通常の運用スケジュールを決定するメトリクス「運用時間（通常）」と、それとは異なる運用スケジュールを決定するメトリクス「運用時間（特定日）」の二種類を定義している。平日の業務運用以外に土曜日のバックアップ運用と日曜日の計画停止といったように、通常の運用スケジュール以外の特定日が複数存在する場合は、それぞれの特定日について確認しておく必要がある。

「保守運用」には、小項目「計画停止」、「パッチ適用ポリシー」、「活性保守」などのシステムの品質を維持するために実施するメンテナンス作業の方針や内容に関する項目を定義している。これらは、メンテナンス作業の方法やスケジュールを左右する項目であり、導入する機器の選定にも大きく影響するため事前に決定しておくことが重要である。

「障害時運用」には、小項目「復旧作業」、「システム異常検知時の対応」、「交換用部材の確保」といった、システム障害が発生した際の対応を決定するための項目を定義している。

「通常運用」の小項目「運用時間」と同様、ここでも小項目「復旧作業」が運用・保守性と可用性で重複項目となっている。導入機器や要員・部材の確保等、コストに大きく影響する項目が多いため、可用性の観点と運用・保守性の観点の双方から十分に検討する必要がある。

「運用環境」には、小項目「開発用環境の設置」、「試験用環境の設置」、「マニュアル準備レベル」や「リモートオペレーション」といったシステム運用を行う環境に関する項目を定義している。これらの項目は、システムの運用方法に大きく影響するものであり、実運用が始まってからもれに気づくケースが見受けられるので注意が必要である。

「サポート体制」には、小項目「保守契約（ハードウェア）」や「保守契約（ソフトウェア）」など保守契約に関する項目や「メンテナンス作業役割分担」、「一次対応役割分担」などシステム運用に関するユーザ/ベンダ間の役割分担に関する項目、そして、「オペレーション訓練」や「定期報告会」といったユーザのシステム運用に対するベンダのサポート体制に関する項目を定義している。これらは、システムの開発や構築には直接関係しないとして検討を後回しにされがちだが、システムの品質を確保するためには事前に検討しておくなければならない項目である。

「その他の運用管理方針」には、小項目「内部統制対応」と「サービスデスク」、「インシデント管理」などの ITIL 関連の項目を定義している。これらの項目は、管理を行うかどうかについて確認する項目となっており、実際に管理を実施することでユーザとベンダが合意した際には、具体的な実現方法について確認する必要がある。システムの設計や開発の作業にも影響する項目であるため、具体的な実現方法も含めて事前に確認しておく必要がある。

2.2.4 移行性

(1) 概要

移行性は、現行システム資産の移行に関する要求である。新システムの稼働に向けて、完全に新規で開発する場合を除き、現行システムの資産を新システムに移行しなければならない。なぜなら資産が移行できなければ、システム開発が完了していてもシステム全体として利用することができないためである。したがって、システム移行に必要な要求項目を抽出して移行計画を策定し、これを確実に実施することが重要である。

移行性は、移行のスケジュールに関する「移行時期」、新システムへの切り替え方式に関する「移行方式」、移行する資産の対象を把握する「移行対象(機器)」、「移行対象(データ)」、および移行のためのリハーサル等を行う「移行計画」の5つの中項目から構成される。

(2) 留意事項

「移行時期」として、移行計画からシステム切り替えまでの期間がどれくらいか、その中で移行作業の際にシステム停止が可能か、並行稼働が必要か、という観点で検討する。並行稼働が必要な場合は、並行稼働の期間についても合意しておくことが重要である。

「移行方式」としては、システムが複数の場所で設置される場合の小項目「拠点展開ステップ数」と、システムが複数業務で構成される場合の小項目「業務展開ステップ数」がある。どちらの場合でも、移行や展開がより多段階になるほど新旧両システムの部分的な共存稼働期間が長くなる。新旧共存のためにシステム全体を継続稼働させる場合、新旧両システムの並行稼働を考慮すると、一斉展開より多段階展開の方が難易度は高い。しかし、対象システムにおける展開時のリスクによっては、一斉展開の難易度が高くなる場合もある。したがって、移行や展開の段階数については、対象システムについて拠点毎、業務毎に展開時のリスクを事前に考慮することが必要である。

移行対象として「移行対象(機器)」と「移行対象(データ)」を確認する。

「移行対象(機器)」では、小項目「移行設備」として旧システムで使用していた設備や機器を新システムでハードウェアだけを入れ替えて使い続けるのか、全く新しいシステムとして入れ替えるのかなど、入れ替えの範囲を確認しておくことが重要である。その際、設備や機器を部分的に入れ替える場合には継続利用するハードウェアやソフトウェアについて、保守サポート可否や入れ替える設備や機器との互換性を考慮する必要がある。

「移行対象(データ)」では、メトリクス「移行データ量」、「移行データ形式」、「移行媒体種類数」、「移行ツールの複雑度(変換ルール数)」などがある。特に移行データでは、データ形式が移行先と異なる場合は形式変換用の設備や移行ツールが必要になる。移行ツールではツールの複雑度として変換ルール数で示しており、変換時のルールが増加するとツ

ール開発量や変換作業時間などに影響するため重要である。また、移行する際に使用しなければならない移行媒体の種類毎に、移行設備にどのように取り込むのか、その方法や装置の検討が必要である。

「移行計画」では、小項目「移行作業分担」、「リハーサル」、「トラブル対処」をそれぞれ確認する。

移行作業のユーザとベンダの分担については、特に移行対象データに関する旧システムの移行対象データの調査、移行データの抽出や変換、本番システムへの導入と確認、等について、その作業分担を規定しておくことが重要である。なお、最終的な移行結果については、ユーザが確認しなければならない。

外部連携リハーサルでは、通常のリハーサルと同様に対象である外部システムを明確にして、リハーサルの範囲、環境、回数について規定することが必要である。さらに外部システムとの接続仕様に変更がある場合には、新システムで新旧両仕様をサポートすることがある。その際にはシステム移行リスクを軽減するために、両接続仕様を確認する外部連携リハーサルを計画することが必要である。

小項目「トラブル対処」とは、移行実施場所に駐在する人員や切り戻しタイミングの対応プラン等をあらかじめ取り決めておく項目である。万一トラブルが発生した場合にスムーズに対応することを目的とするものであり、その内容を確認しておくことが重要である。

2.2.5 セキュリティ

(1) 概要

セキュリティは、構築する情報システムの安全性の確保に関する要求である。適切なセキュリティ対策が講じられないと、脅威が現実のものとなり、情報システムを用いた業務の遂行に支障が生じ、その結果として直接的、間接的に大きな社会的・経済的損失がもたらされるおそれがある。そのため、構築する情報システムに応じて検討すべきセキュリティに関する非機能要求を明らかにし、抜け漏れが生じないように検討する必要がある。

また、セキュリティに関する非機能要求は、情報システムの性能に影響を与える要求が多い。例えば、暗号処理のように元の情報処理に負荷を加えるような要求が多いためである。セキュリティに関する非機能要求を検討する際には、併せて性能・拡張性に関する非機能要求を検討することが重要である。

セキュリティは、対象システムのセキュリティに関する前提条件・制約条件である「前提条件・制約条件」、開発時や運用時のセキュリティ管理に関する項目である「セキュリティリスク分析」、「セキュリティ診断」、「セキュリティリスク管理」、セキュリティ対策を実現するための機能である「アクセス・利用制限」、「データの秘匿」、「不正追跡・監視」、機能の組合せによるセキュリティ対策の主要なパターンとなる「ネットワーク対策」、「マルウェア対策」、「Web 対策」、セキュリティインシデント発生時の対応等に関する項目である「セキュリティインシデント対応/復旧」の中項目から構成される。

(2) 留意事項

「前提条件・制約条件」は、情報システムに対するセキュリティ対策を実施するにあたり、主に法令や、業界における情報セキュリティに関する基準⁴、ガイドライン、企業における情報セキュリティポリシーといった組織規程などの確認に関する項目である。「前提条件・制約条件」となる規程、法令、ガイドライン等を確認し、それらの条件に従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。例えば、順守する規程等により、小項目「認証機能」、「データ暗号化」などに該当する明確なセキュリティ要件が定められている場合がある。このような場合、それらの規程等により示されているセキュリティ要件と、選択したレベルとの間に矛盾が生じないように非機能要求を決定する必要がある。なお、モデルシステムでは、セキュリティに関する業界の基準や企業方針などの影響を受けない汎用的な例を示しているため全て規程がない例を示している。そのため、グレード表の「E.1.1.1 順守すべき社内規程、ルール、法令、ガイドライン等の有無」のベース値は、全てモデルシステムにおいてレベル 0（無し）としている。業界の基準や企業の方針に応じて、順守すべき規程、法令、ガイドライン等があるかを確認し、ある場合はそれらを満たすようにレベルを決定する必要がある。

⁴ 「政府機関における情報セキュリティ対策のための統一基準」、「金融機関等コンピュータシステムの安全対策基準」、「Payment Card Industry Data Security Standard (PCI DSS)」などがある。5.2.6 項～5.2.8 項を参照のこと。

「セキュリティリスク分析」は、情報システムを開発するにあたり、潜在する脅威を洗い出し、セキュリティ対策の実施範囲を明確にするためのリスク分析に関する項目である。

「セキュリティリスク分析」について検討する際には、情報システムで取り扱う資産（ハードウェア・ソフトウェア資産および情報資産）を洗い出し、どの資産が保護対象かを確認しておく必要がある。また、セキュリティに関する非機能要求を合意する際には、項目一覧に示されたセキュリティ対策の実施の有無だけでなく、セキュリティ対策を実施しない項目については対策を実施しないことにより残存するセキュリティリスクも合意する必要がある。

「セキュリティ診断」は、開発する情報システムに対してセキュリティに特化した試験の実施について合意するための項目である。「セキュリティ診断」について検討する際には、利用するツールやレビュー方法等、より具体的な診断方法や診断範囲についても検討する必要がある。

「セキュリティリスク管理」は、システム運用後に発見された脅威や脆弱性への対応方針について合意するための項目である。「セキュリティリスク管理」は、セキュリティパッチの適用範囲やタイミング等に関する項目を含むため、運用・保守性にあるパッチ全体の適用範囲やタイミングに関する項目と併せて検討する必要がある。

「アクセス・利用制限」は、開発する情報システムで取り扱う資産に対するアクセスおよび利用の制限について合意するための項目である。「アクセス・利用制限」について検討する際には、実施箇所（サーバ、ストレージ等）毎に対策の検討を行う必要がある。

「データの秘匿」は、開発するシステムにおいて流通および蓄積する情報の秘匿の実施について合意するための項目である。「データの秘匿」について検討する際には、秘匿対象とする情報資産および実施箇所について併せて検討する必要がある。秘匿するために暗号処理を行う場合は性能への影響を考慮する必要がある。

「不正追跡・監視」は、システム運用後に発生する不正行為の追跡および監視について合意するための項目である。「不正追跡・監視」について検討する際には、不正行為を検知するためのセキュリティログの取得等による性能への影響を考慮する必要がある。

「ネットワーク対策」は、ネットワークへのセキュリティ対策について定義した項目である。「ネットワーク対策」では、不正な通信を遮断するための制御やシステム内の不正行為や通信を検知する仕組みの導入、そして、ネットワークを介した攻撃による輻輳への対策を

検討する。輻輳対策として、サーバ処理能力の増強で対処する場合、性能・拡張性の中でサーバの処理能力を決めていくリソース拡張性などの項目と併せて検討する必要がある。

「マルウェア対策」は、コンピュータウイルス、ワーム等のマルウェアへのセキュリティ対策について定義した項目である。「マルウェア対策」について検討する際には、リアルタイムでのマルウェアの検知等を行うことによる性能への影響を考慮する必要がある。

「Web 対策」は、Web アプリケーションの脆弱性へのセキュリティ対策について定義した項目である。「Web 対策」について検討する際には、WAF（Web Application Firewall）によるリアルタイムでの監視を行うことによる性能への影響を考慮する必要がある。

「セキュリティインシデント対応/復旧」は、セキュリティインシデントが発生することを前提とした対策について定義した項目である。「セキュリティインシデント対応/復旧」では、セキュリティインシデント発生時の対応等だけでなく、インシデント対応マニュアルの整備やセキュリティ教育等も併せて検討する必要がある。

2.2.6 システム環境・エコロジー

(1) 概要

システム環境・エコロジーとは、システムの設置環境やエコロジーに関する要求である。前者のシステム環境の部分は、システムが設置される際の約束事である「システム制約/前提条件」やシステムを取り巻く利用者や地域的な広がりなどの「システム特性」、「適合規格」、「機材設置環境条件」から構成される。こうした項目は、後から規定があることがわかっても容易には変更することが困難であるため、定義の漏れがあると要件定義の手戻りなどが発生し大きなトラブルの要因となりやすいため重要な項目である。

また、後者のエコロジーの部分は、「環境マネジメント」から構成される。主なものに廃棄物量や CO₂ 排出量の低減、エネルギー消費効率の向上などがある。近年、世界的にも CO₂ 削減の義務化や規制方針が打ち出されている国や地域もあり、重要な項目となってきた。

(2) 留意事項

「システム制約/前提条件」には、小項目「構築時の制約条件」、「運用時の制約条件」の2つを定義している。構築時および運用時に制約条件となるような組織内の規定や法令・条例などが存在していれば、それに準拠させる検討が必要である。これらを意識せずにシステムを構築した場合には、改めて規定に準拠するような構成へ変更したり、条件を満たすような再設計が必要になったりするケースもある。例えば、入退室管理に関する規定などがあり、これに従ってデータセンターに設置されたシステムで、運用時にはリモートからの操作が必要にもかかわらず、要件定義段階でこうした条件が漏れていた場合などがこのケースにあたる。

「システム特性」には、小項目「ユーザ数」、「クライアント数」、「拠点数」、「地域的広がり」、「特定製品指定」、「システム利用範囲」、「複数言語対応」を定義している。ユーザ/ベンダ間で早期に共通認識を持つておくことが、システムを構築していく上で非常に重要である。なぜならば、これらの項目はシステムの規模や特性を決定づける要件となるからである。例えばユーザ数やクライアント数などが正しく定義されていなかったり、システムのライフサイクルの中で将来の増大の考慮がもれていたりすれば、リソースの問題を引き起こす可能性もある。これらの項目は、早期に合意を図っておくことにより、システムの特性をおさえやすくなる。

「適合規格」には、小項目「製品安全規格」、「環境保護」、「電磁干渉」の3つを定義している。システムの用途や設置環境・運用環境によっては、製品が一定の基準を満たしていることを求められる。製品の安全性や機器が発生する電磁波への規制、また特定有害物質の使用制限規制などが要求に含まれる場合もあるので、構成する機器への要求を確認しておく。

「機材設置環境条件」には、小項目「耐震/免震」、「スペース」、「重量」、「電気設備適合性」、「温度（帯域）」、「湿度（帯域）」、「空調性能」の7つを定義している。これらの項目は、要件定義段階で定義から漏れやすい項目である。例えば、要件定義段階から設置環境についても十分に検討しておかないと、いざ設置しようとしたときに、フロアの荷重条件を満たさなかったり、スペースの関係上設置できなかったりといったケースも考えられる。

「環境マネジメント」には、エコロジーに関する小項目「環境負荷を押さえる工夫」、「エネルギー消費効率」、「CO₂排出量」、「低騒音」の4つを定義している。エコロジーに関して、最近では官公庁を筆頭にグリーン調達を行う企業が増えてきている。また、今後は炭素税など法的な対応によって大きくクローズアップされてくる可能性も出てきている。更にエコロジーには、企業の社会的責任（CSR）や公正で透明かつ健全なビジネスを体現するとの視点もあり、企業が社会の信頼を得る上で今後益々重要性が高まると考えられる。

3 FAQ

【非機能要求グレードのスコープ】

Q1: 非機能要求グレードとして、なぜこの 6 大項目が選ばれたのか？

A1: システム基盤を定める際に確認したいユーザの要求について、各種標準類や事例といった知見をボトムアップに集約、整理し、現在の 6 大項目に分類しました。その際、ISO/IEC 9126 などの標準類についても参考にしていますが、非機能要求グレードは主にシステム基盤が実現する非機能要求にフォーカスしているため、それら標準類の全ての項目は網羅しておりません。

Q2: アプリケーションへの要求は非機能要求グレードのスコープに含まないのか？

A2: 機能要求は主に業務やアプリケーションによって実現され、非機能要求は主にシステム基盤と呼ばれる領域によって実現されます。システム基盤とは、サーバやストレージ、ネットワークなどのハードウェア機器、あるいは OS、ミドルウェア、その他の制御や運用管理を行うソフトウェアなどを指します。「非機能要求グレード」では、このシステム基盤が実現する非機能要求を対象とし、業務やアプリケーションが実現する機能要求に関してはスコープ外としました。しかし、実際のシステム案件における要求検討においては、システム基盤とアプリケーションの境界が明らかではなく、それらを合わせて検討しなければならないケースも存在すると認識しています。そのため、一見業務やアプリケーションに含まれると考えられる項目についてもシステム基盤の検討を行うために必要なものはスコープに含めています（例：業務処理量、運用時間など）。

Q3: なぜ、「グレード」という言葉を使ったのか？

A3: 「グレード」は、システムの実現レベルの段階的な差を示し、システムの仕様となる要求事項のセットを同時に満たす用語を探してつけたいわばコンセプト用語です。特に優劣を示すことを意図した用語ではなく、自動車というラグジュアリー・グレード、エコノミー・グレード、スポーツ・グレードといった考え方に似ており、どれも特定の要望にあったものであることを意図しています。

情報システムは、それを構成する要素となるハードウェア・設備、OS・ミドルウェア、運用管理の仕組み・体制などの組合せと連携により実現水準には差があるものの、開発初期にはその差がユーザからは認識されにくく、ベンダとしても技術を説明するのが難しいという課題があります。このような状況下、システム間の差を「グレード」として段階的に示し、早期にユーザとベンダ双方で要求事項の確認ができる仕組みを検討することを目的に「非機能要求グレード」を作成しました。

Q4: 非機能要求グレードが対象としているユーザは？

A4: 非機能要求グレードは、情報システムの開発プロセスにおいて要件定義などの場面で非機能要求を提示、提案、決定することにかかわる発注者、受注者双方の担当者を対象としています。また文中では、発注者をユーザ、受注者をベンダと統一して呼んでいます。具体的には、「経営者が参画する要求品質の確保第 2 版 (SEC BOOKS)」を参考として、発注者企業における情報システム部門をユーザに想定しています。ただし、これは利用ガイドにおいて利用方法を客観的に説明するための便宜上の設定であり、非機能要求グレードを、誰が、どのように利用するかということを制限するものではありません。

Q5: 非機能要求グレードはシステムライフサイクルのどの時点で使うものか？

A5: 非機能要求グレードは、「共通フレーム 2007」における企画プロセス、要件定義プロセス、開発プロセスの中で非機能要求を扱うプロセスやアクティビティで活用されることを想定しています。また、「経営者が参画する要求品質の確保第 2 版 (SEC BOOKS)」においては、「システム化の方向性」、「システム化計画」、「要件定義」といった上流工程がそれにあたります。非機能要求グレードは、ユーザ/ベンダ間で非機能要求について合意を行うためのツールであり、その内容は、RFP、要件定義書、見積り提案といった文書に記載されたり、システム設計契約として合意事項に含まれることを想定しています。なお、主に上流工程での利用を想定していますが、「非機能要求グレード」により整理された内容はシステムの設計や試験においても利用可能と考えられるので、必要に応じてご利用いただければと考えています。

【グレード表、項目一覧および樹系図】

Q6: 項目一覧のレベルは何の順番で並んでいるのか？

A6: メトリクスが通常取りうる値をレベル 0 からレベル 5 までの 6 段階に整理しました。レベルが大きいほど難易度が高く、一般に開発コストが高くなることを示しています。隣り合うレベル値の間には、アーキテクチャのギャップが存在するように設定されており、レベル値を上げたり下げたりすると、その結果の要件を満たすシステムを設計・実装する際に何らかの構造的変化が現れると考えられます。ただし、一部のメトリクスについてはレベルが 0 または 1 の二値で表現されているものが存在しています。これらは、法的な制限の有無などを表現する単純二値であったり、具体的な値が定まっていない場合のリスクを想定するリスク順を示したりするものとなっています。これらは、レベル値間におけるアーキテクチャのギャップが明確でなく開発コストへの影響が実感しにくい、制限が存在したり、リスクが高い方が実現の難易度が高く、結果として高コストになる可能性が高いとしてレベル順序を決定していま

す。

Q7: 大項目間で同じメトリクスが存在しているが、それらはどう考えればよいのか？

A7: 非機能要求グレードでは、大項目毎に検討対象者や検討順が異なることを想定し、検討漏れを防ぐために、いくつかの項目が重複して存在しています。それらには別々の値を設定するのではなく、同じ値が入るようにします。複数の担当者が大項目毎に検討した結果をマージする場合や、時間的に離れたタイミングで各大項目を検討するような場合には、重複項目列に○印がついている項目について、大項目間の整合をとって検討を進めるようにしてください。

Q8: 「運用コストへの影響」は何を表しているのか？

A8: 項目一覧またはグレード表のレベルは開発コストの高低を表していますが、システム開発では、開発コストだけでなく運用コストも含めたトータルコストで評価しなければなりません。開発コストとは要件定義後からシステムが出来上がってサービスインするまでの期間にかかるコストのことであり、運用コストはサービスイン以降にシステムを維持・管理していくために発生するコストのことです。項目一覧で定義されている要求項目には、処理の自動化などのように開発コストをかけることによって運用コストを下げられる項目があります。そのような開発コストと運用コストがトレードオフの関係となる可能性のある項目について「運用コストへの影響」欄に○印を付けています。したがって、開発コストの高いレベルを指定してもトータルコストを抑えられるケースがあります。

Q9: グレード表の対象項目である重要項目の選択根拠は？

A9: 非機能要求グレードの項目一覧には、238 のメトリクスが存在します。これらのメトリクスには、決定順序が異なるものやシステム基盤のコストに対する影響度合いが異なるものなどがあり、何らかのグルーピングが必要です。一方、単純に項目数が多すぎて検討に時間がかかるといった問題も考慮し、重要項目を選定しました。重要項目の選定にあたっては、システムの開発コストや品質に影響を与える度合いが大きい項目を、ユーザ視点とベンダ視点の両方から評価しました。

Q10: 樹系図は何を表しているのか？

A10: 樹系図は、グレード表や項目一覧の閲覧性を高めるためものです。樹系図上の項目は、ユーザ/ベンダ間で調整が進んでいく順序を大まかに示すように左上から右下に向かって配置されています。厳密な定義はしていませんが、左から右への流れは大まかに中項目の流れを示し、上から下の流れは各小項目の検討順を示しています。このように、「中項目」、「小項目」、「メトリクス」の系統図で検討順を示したという意図

で、一般的な「樹形図」の文字を用いずに「樹系図」の表記を使用しています。

【非機能要求グレードの利用方法】

Q11: 項目数が多すぎて一度に検討しきれないが、どうすればよいのか？

A11: 項目一覧の中からより重要度の高いメトリクスを選別し、それらから検討を開始できるようグレード表を定義しました。グレード表では、重要度の高いメトリクスに絞り込んだだけでなく、モデルとなるシステムを想定してレベル値の選択例（ベース値）も示しています。検討の手順としては、グレード表のモデルシステムをひとつ選定し、各メトリクスの選択レベルを調整することで、目的のシステムへの要求に近づけていくという方法があります。

Q12: 自分の検討するシステムとは無関係の項目が存在するが、どうすればよいのか？

A12: グレード表と項目一覧は、システム開発にあたって必要な項目を抽出しています。要件定義工程における RFP や見積提案に記載されて、その時点における合意事項に含まれます。ユーザの環境や対象となるシステムによっては検討不要となる項目も出てくることが想定されますが、その場合には検討しない理由をユーザとベンダの間で合意する必要があります。

Q13: 契約時点では決定できない項目が存在するが、どうすればよいのか？

A13: 非機能要求グレードでは、要件定義工程において項目一覧の全項目を合意することが望ましいと考えています。しかし、詳細な設計後でなければ決められないなどの理由で必ずしも上流工程で全要求項目が決定できるとは限りません。決定できない項目に関して決定時期や決定方法などを明確にしておく必要があります。このような場合には、契約変更や多段階契約を考える必要があります。

Q14: 開発プロセスの途中で要件の変更があった場合、どうすればよいのか？

A14: 非機能要求グレードは、要件定義工程において利用されることを想定していますが、そこで決定された内容がきちんとシステム設計や構築内容に反映されているかをチェックするような用途にも利用できると考えています。そういった開発プロセスの途中において要件を変更する必要がある場合も十分に考えられます。その際の要件変更の内容やその影響度合いをユーザとベンダの間で確認・合意するためのツールとして非機能要求グレードが利用できると考えています。

Q15: ツールの利用に何か条件はありますか？

A15: 「利用編」と「解説編」の 2 編の利用ガイドと、「グレード表」、「項目一覧」、「樹系

図」の3つのツールの著作権は独立行政法人 情報処理推進機構（以降、IPA）が保有しています。IPAは、これらツールを広く世の中で利用していただくことを希望しており、著作権を維持するための最低限の使用条件を設けた上で、自由にご利用いただけるように公開しております。また、項目一覧とグレード表を1つの編集可能なスプレッドシートの形式にした「活用シート」も提供しています。

詳細な使用条件については、個々のガイドとツールの記載をご参照ください。

4 用語集

	用語	説明
【あ】	移行設備	システム基盤を構成する設備の中で、新たな設備に入れ替え対象となる設備。
	移行データ形式	アプリケーションに依存したフォーマット、テーブル形式や文字コードなど、新システムに移行するために考慮すべきデータ形式のこと。
	移行媒体種類数	現行システムのデータを新システムに移す場合に、使用しなければならない媒体種類の数。例えば、テープ、ディスク、伝票類など。また、ネットワーク接続によるデータ転送も媒体種類として含む。
	一次対応	情報システムあるいはそれを構成する各機器やソフトウェア等の障害問い合わせ窓口が行う初動調査のこと。主に情報収集や問題切り分けを担当する。
	インシデント	情報システムにおいて、サポート担当者が対応すべき障害や問題点などの単位。
	運用サイト	稼働するシステムを設置する場所。
	エネルギー消費効率	「エネルギーの使用の合理化に関する法律」（略称：省エネルギー法）に於いて、同法で定める測定方法により測定した消費電力を複合論理性能で除したものと定義(従って、得られた値が小さいほど効率が良い)。同じ能力を得るのに必要なエネルギーが少ないほどエネルギー消費効率は良くなる。
	エラー監視	システムを構成するサーバやその他の機器、あるいはその上で稼働するミドルウェアやアプリケーション等が規定するログファイルへのメッセージ出力からエラーの発生を検知する監視方式。
	エラー検出	データの完全性を保証する機能の1つであり、データの誤りを検出する機能のこと。 (関連用語) → データインTEGRITY
	エラー訂正	データの完全性を保証する機能の1つであり、検出したデータの誤りを訂正する機能のこと。
	オペレーション	情報システムに対する一連の操作のこと。
	オペレーション訓練	システムの操作に関する訓練のこと。
【か】	回線	ネットワークを構成する伝送路のこと。
	回復性	障害が発生した際に、要求された水準までシステムを復旧するための能力。
	外部システム	開発対象のシステムの範囲外に存在するシステムのこと（開発対象のシステムと連携する既存システムなど）。
	外部データ	外部システムが保有するデータのこと。開発対象のシステムが保有するデータの集計元であったり、複製である場合もある。
	鍵管理	暗号、デジタル署名等で用いる鍵の管理。
	火災対策	火災によるシステムへの被害を防ぐための対策。検知対策、消火対策などがある。
	活性保守	情報システムを構成する機器の追加、削除や部品交換をシステムが稼働したままの状態で行うこと。
	稼働時間	システムが1日の中でサービスを提供する時間。運用時間。
	稼働率	システムがサービスを提供する予定だった時間のうち、実際にサービスを提供できた時間の割合。運転時間率。逆にサービスを提供できなかった時間は、平均ダウン時間として表される。また一般的に稼働率は、以下の式で表わされる。 稼働率=MTBF/(MTBF+MTTR) (関連用語) → MTBF(平均故障間隔)、MTTR(平均復旧時間)
	雷対策	雷による過電流からシステムを守るための対策。

用語	説明
可用性	(1) システムが明示された利用条件の下で、定められた時点に、要求された業務をどの程度実行できる状態であるかを示す能力。大項目名として用いる可用性は、信頼性を含めた意味で定義している。 (2) 許可された対象（ユーザやプログラム）によって要求されたときにアクセスと使用が可能な特性。
ガル (Gal)	加速度を表すためのCGS単位(1Gal＝1cm/ (sec ²))。落体の法則を発見したガリレオ・ガリレイにちなんで名づけられた。例えば、地表での重力加速度は約980Galである。なお、地震震度との対応関係は、震度4(25～80Gal)、震度5(80～250Gal)、震度6(250～400Gal)、震度7(400Gal以上)といわれている。
監視	情報システム自体やそれを構成する機器、プログラム等、対象物が期待する状態にあるかどうかを確認し、指定された通知先へ確認した内容に基づいた通知を行うこと、またはその仕組み。 (関連用語) → 死活監視、エラー監視、リソース監視
機材設置環境条件	機材を設置する建屋側が提供可能な環境。具体的には、許容される機材の重量やスペース、電気設備適合性、温度、湿度、耐震/免震対策などがある。
機密性	ある情報へのアクセスが許可されていない対象（ユーザやプログラム）に対し、その情報を利用不可もしくは非開示にする特性。
脅威	セキュリティリスクを引き起こす可能性を持つ、システムへの攻撃、きっかけ、操作・設定ミス等。
業務	システムが有する機能を利用し、与えられた要求を処理すること。システムが有する機能だけでなくシステムの利用や人による活動を含む。
業務機能数	対象業務を構成する機能を（機能構成図や機能情報関連図等により）洗い出した数。サブシステム数や画面数などでも代用可。
業務継続性	災害や故障など予期せぬ事象が発生しても、稼働可能なリソースの活用や、瞬時の復旧をもって、業務を継続する能力。BCP（Business Continuity Plan）。
業務継続の要求度	発生する障害に対して、どこまで業務を継続させるかを示す度合い。
業務展開ステップ数	システムが複数業務で構成される場合、段階的に業務を新システムへ移行や展開をするときの展開段階数。例えば、3つの業務サブシステムからなる基幹業務システムを、A業務、B業務、C業務という順番で移行を実施すると、業務展開ステップ数は3段階となる。
共用センタ	大規模災害時に、自システムでの復旧が不可能な場合に利用できる共用のデータセンター、サーバー群。
拠点数	サービスを提供するためのシステムが展開される場所の数。一般には、支社、支店、店舗、工場などシステムの機材が設置される拠点の数を指す。
拠点展開ステップ数	システムが複数の場所で設置される場合、段階的にシステム基盤やデータを新システムへ移行や展開をする時の展開段階数。例えば、本社と支社で使用する基幹業務システムを、本社、支社A、支社Bという順番で移行を実施すると、拠点展開ステップ数は3段階となる。
クライアント数	サービスの要求を行う側の端末の数。
クラスタ	システムの信頼性あるいは処理性能の向上を目的とし、複数のコンピュータを1つにまとめる構成のこと。コールドスタンバイやホットスタンバイなどの方式がある。
グリーン購入法	「国等による環境物品等の調達の推進等に関する法律」の略称。製品やサービスを購入する際に、環境を考慮し、必要性をよく考え、環境への負荷ができるだけ少ないものを選んで購入することをグリーン購入といい、国等の機関にグリーン購入を義務づけるとともに、地方公共団体や事業者・国民にもグリーン購入に努めることを求めている。グリーン購入は、消費生活など購入者自身の活動を環境にやさしいものにするだけでなく、供給側の企業に環境負荷の少ない製品の開発を促すことで、経済活動全体を変えていく可能性を持っているとしている。
グレード	1つのモデルシステムに対する非機能要求の選択レベルと選択時の条件のセットのこと。
グレード表	システム基盤の非機能要求非機能要求に関するグレード表のこと。非機能要求グレードでは3つのモデルシステムのグレード表を提供している。
計画停止	保守や点検などを目的にあらかじめ予定された情報システムの停止のこと。反対に、障害などにより意図せず発生する情報システムの停止を計画外停止と呼ぶ。
経路	ネットワーク内をデータが流れる際の順路のこと。

【さ】

用語	説明
コンポーネント	装置を構成する部品。例えば、サーバであれば、CPUやディスク、ネットワークカードなど。
サーバ監視	情報システムを構成するサーバあるいは、サーバ機能を提供するソフトウェアの監視。ノード監視。
サービス	システムが提供する便益。システムとはITシステムのことを言う。
サービス切替時間	システムをクラスタなどにより冗長化させた際に、一方から他方へサービスを切り替えるまでの時間。ダウンタイムと同等。 (関連用語) → 稼働率、MTTR
サービス停止攻撃	サーバサービスに対して、大量のパケットやデータを送付して、回線容量、メモリ容量などを消費させたり、CPUを過負荷状態にして、サービスやシステムの処理能力を低下させたり、ダウンさせたりすること。
サービスデスク	情報システムのメンテナンスを実施し、その利用者に対して日々の運用であるサービスサポートを提供する組織機能のこと。
再試行	データの完全性を保証する機能の1つであり、データの誤りを検出した際に、処理を再実行する機能のこと。例えば演算器やレジスタなどのハードウェアでの命令の再実行など。 (関連用語) → データインテグリティ
死活監視	監視対象が起動しているかどうかについての確認を行う監視方式。
時間指定回復	バックアップを用いたデータの復旧作業において、特定の期間内の任意の時点にデータの内容を回復できる機能のこと。Point in Time Recovery (PITR)。
資産	システムに関連する、ハードウェア、ソフトウェア資産、情報資産および業務。
地震対策	地震によるシステムへの被害を防ぐための対策。耐震、免震、制震などの対策がある。 (関連用語) → 耐震、免震
システム	主に、ハードウェア、ソフトウェア、その他設備の総称のことを言う。ITシステムと同義。広義のシステムは人間系も含めるが、非機能要求グレードでは人間系を含めない狭義のシステムとして用いる。
システム移行期間	現行システムから新システムへの移行のための作業計画から新システムが本格稼働するまでの期間のこと。
ジャーナルログ	システムに障害や処理の異常などが発生した際における原因の究明や復旧を目的として保存される処理の履歴、記録。
遮断対策	漏電対策において、検知した漏洩電流がシステムへ流れるのを防ぐ対策。
重複項目	大項目間で重複する項目。グレード表や項目一覧では重複項目列に○を付けている。
重要項目	システム基盤の非機能要求を検討する上で品質やコストに大きな影響を与える項目。項目一覧では重要項目列に○を付けており、樹系図ではメトリクスに網掛けを行っている。
瞬電・停電対策	停電や瞬間的な停電である瞬電などが発生した際に、電力の安定供給を行えるようにするための対策。
障害時運用	システムの内部、あるいは連携している外部システムに障害が発生している状態を想定して設計された運用方法のこと。
障害パッチ	製品不具合を改修するためのパッチのこと。
処理余裕率	単位時間で処理したい件数の何倍まで対応可能とするかを示す目標値。（余裕率を大きく設定すると過剰投資になり、小さく設定すると、想定以上の件数に対応できなくなる） 通常時処理余裕率＝（通常時単位時間あたり処理件数）／（単位時間あたり処理件数） ピーク時処理余裕率＝（ピーク時単位時間あたり処理件数）／（単位時間あたり処理件数） 縮退時処理余裕率＝（縮退時単位時間あたり処理件数）／（単位時間あたり処理件数）
冗長化	正常時には一つあれば十分な機能ユニットを異常時に備えて複数用意し、異常時に代替動作ができるように予め構成または計画しておくこと。

用語	説明
情報セキュリティポリシー	組織のセキュリティに関する方針を示したもの。一般的に、方針では、情報セキュリティに関する目標（どこまで守るか）と目標達成のために組織が実施すべき行動や責任者の明確化等が含まれる。これらの情報セキュリティポリシーを基に、実施すべき対策の基準、また、それらを実施する際の手順が策定されることとなる。
スキルレベル	情報システムを構成する業務機能や製品に対する習熟度。
スケールアウト	サーバの処理能力を向上させるためのアプローチの1つ。複数のサーバを並べシステム全体としてサーバの処理能力を向上させる。
スケールアップ	サーバの処理能力を向上させるためのアプローチの1つ。CPUを追加したり、高性能のものに置き換えることによりサーバの処理能力を向上させる。
ストレージ	システムを構成する要素の1つで、データを記憶するための装置のこと。
スパイク負荷	通常時の負荷と比較して、非常に大きな負荷が短時間に現れること（業務量の想定されたピークを超えた状態）。特に一般ユーザ向けシステムなどクライアント数を制限できないシステムで発生しやすい。
スループット	システムが単位時間あたりに処理することができる仕事の量。システムの処理能力の指標となる。
脆弱性	セキュリティ対策を実現しても考慮しなければならない可能性や原因（攻撃の可能性、運用ミス、利用者の不注意、ルール違反等）。
性能品質保証	性能要件を満たすために、あるいは作りこむために必要な項目。
セキュアコーディング	ソースコードに脆弱性を含まないように実施するプログラミング方法。
セキュリティ	本グレード標準では、システムが保有する情報資産を安全に守る、「情報セキュリティ」の意味で用いる。広義の「セキュリティ」には、安全性（身体や物に損傷、損害がない状態）の意味も含まれるが、本グレード標準ではこれを含めない。
セキュリティパッチ	パッチのうち、特にセキュリティホールを修正するパッチのこと。
セキュリティリスク	システムや守るべき資産にとって、起こるべきでない状況や状態。
セキュリティリスク対策	情報セキュリティを保つための技術もしくは運用による実現手段。
セキュリティリスク分析	想定するセキュリティリスクやセキュリティの脅威を洗い出し、分析すること。
セグメント分割	用途やシステムの形態に応じて複数の領域に分けてネットワークを構成すること。
世代管理	定期的にバックアップをとる際に直近のデータだけでなく、過去のデータも保管しておき、それぞれからデータ復旧をすることができるバックアップの管理方式。
選択レベル	モデルシステムを想定して選択したレベルのこと。レベル値とレベルの説明から構成される。 （関連用語） → ベース値
ソフトウェア配布	ソフトウェアの障害パッチやバージョンアップファイルなどを情報システムを構成する機器に配布すること。
【た】ターンアラウンドタイム	システム等にリクエスト（要求）を送信してから結果が返ってくるまでの時間。 （関連用語） → レスポンス
帯域保証	帯域とはネットワーク上の速度のことで、システム（ネットワーク）利用者に対して一定の通信速度を保証すること。
大規模災害	地震、台風などによる自然現象や、テロなどの人為的な破壊行為により発生する災害。直接システムが倒壊するか、電力、水道などのライフラインの停止が余儀なくされることにより、システムの業務継続が困難となる。
耐障害性	障害に対して、指定された稼働水準を維持するための能力。障害許容性。
耐震	ラックを固定するなど、地震による揺れからコンピュータ機器を保護する対策。
代替業務運用	障害でシステムあるいはサービスの一部がシステム上で復旧不可能な場合に、代替でカバーすることが可能な運用手段。

用語	説明
単一障害	システムを構成する要素のうち、冗長化した要素において、一部に障害が発生すること。一重障害。その他で代替することで、業務は継続可能な状態である。
通常運用	情報システムがすべて正常な状態にあることを想定して設計された運用方法のこと。
定期保守	定期的に実施するメンテナンス作業のこと。消耗品の保全交換といったハードウェアのメンテナンスやディスク上の不要ログの削除といったソフトウェアのメンテナンスがある。
ディスク利用率	ディスクに保存されるデータ量が、ディスク全体容量の何割まで使っているかの割合。 ディスク利用率＝（ディスクの使用量）／（総ディスク容量）
データインテグリティ	データがすべて完全に揃っていることを保証すること。データに対して操作が正しく行えること、操作に対して期待した品質が得られること、またデータへの変更が検知可能であることなどを保証する。データ完全性。
データ復旧	情報システムで発生した障害により失われたデータを回復すること。
適合規格	製品が準拠している国際規格、国内規格、海外規格など。
デジタル署名	電子文書の正当性を検証するために付与される情報および用いる技術（デジタル署名を用いることにより、署名者の特定、改竄の検知等が可能となる）。
デフラグ	データの記憶領域内で発生した空き領域の断片化を、データの再配置を行うことで解消すること。
電界・磁界対策	電界、磁界によるシステムへの影響を防ぐための対策。
電気設備適合性	設置予定場所の電源設備諸元(電源容量/電圧/回路数など)に対する導入機器の適合度合い。例えば、100V AC電源可、省消費電力対応などの機材の場合は、一般的に適合性が高いと判断できる。
同一機材拡張余力	既導入済み機材を廃棄することなく、単純な構成要素の追加、増設などによって、性能・容量を拡張できること。なお、契約上はアップグレード可能でもボックススワップなどが必要な場合は当余力が低いと判断する。
導入サポート	システムに製品を導入するにあたり、主に製品の利用方法、構築などを支援すること。
【な】二次対応	一次対応後に実施する対応のこと。二次対応としては、障害部位判別、その部位の障害要因追及、修正、確認及び暫定回避策策定などがある。
二重障害	システムを構成する要素のうち、冗長化している要素で、既に単一障害となった状態で、さらに同要素で障害が発生すること。障害が発生した要素が二重化の場合は、業務停止となる。
認証機能	ユーザや機器等を、識別情報を基に確認するための機能。
ネットワーク機器	システムを構成するLAN、および外部との接続で利用される機器。スイッチ、ルータなど。
ネットワーク診断	診断対象のサーバおよびネットワーク機器等に対して疑似的に攻撃を実施することにより、脆弱性を分析すること。
【は】バックアップ	データの喪失に備えて、別媒体へ復旧可能な状態を保存すること。
パッチ適用	パッチの組込から動作確認までの一連の作業を行うこと（パッチを導入するだけでなく、検証作業も含まれる）。
ピーク時	単位時間あたりの処理量増加等により、システムに最大負荷がかかる時。
輻輳（ふくそう）	通信やその処理に重大な影響を与える多数のアクセス等が集中すること。
付帯設備	サーバを設置する建屋を含め、電源やラックなど、システムに付帯する設備。
復旧作業	復旧作業 障害発生後、システムを要求された水準まで復旧するための作業。
フロア設置用機材	単体で直接床面に設置するように設計された機材。フロアスタンド型、ペディスタル型、タワー型などと呼ばれることもある。
並行稼働	新システム、並びに現行システムの両方を並行して稼働させる状態のこと。
ベース値	選択レベルと同じ。

	用語	説明
	別地保管	バックアップデータを情報システムが存在する場所とは距離的に離れたところへ保管すること。
	変換ルール	移行対象データを新システムへ移行する際に、変換が必要となるルール。この変換が必要なデータ量やルール数により、開発や移行の作業量が大きく異なる。
	保管場所分散度	外部データを保管する場所が、どれだけ分散しているかを示す度合い。
	保守員	保守運用や障害の一次対応における現地作業を担当する人員のこと。
	保守運用	システムを正常な状態に維持するために必要な作業を実施する運用のこと。 (関連用語) → 通常運用、 障害時運用
	保守部品	ハードウェアのための交換部材のこと。
【ま】	マルウェア	コンピュータウィルス、ワーム、スパイウェア等の悪意のあるソフトウェアの総称。
	メトリクス	何かを客観的に測定・計測可能な、具体的で標準的な尺度（指標）のこと。非機能要求グレードでは、各項目をレベル付けする際に、レベルが客観的に判断可能である具体的な指標のことを指す。
	メモリ利用率	システム上でOSやアプリケーションが処理をする際にメモリを使用している割合。 メモリ利用率＝（利用中のメモリ量）／（全メモリ量）
	免震	機器に加わる地震の揺れ自体を低減する対策。
	目標復旧時間	業務停止を伴う障害が発生した際、RPOおよびRLOで設定した目標値に対して復旧するまでに要する目標時間。RTO。実際に復旧のために要した時間の合計値は、平均復旧時間（MTTR）として稼働率の計算に利用する。
	目標復旧水準	業務停止を伴う障害が発生した際、何をどこまで、どれくらいで復旧させるかの示す目標、指標。RTO/RPO/RLOをまとめたもの。
	目標復旧地点	業務停止を伴う障害が発生した際、バックアップしたデータなどからシステムをどの時点まで復旧するかを定める目標値。RPO。
	目標復旧レベル	業務停止を伴う障害が発生した際、どこまで復旧するかレベル（システムのための復旧か、すぐにも業務が再開できる状態か）の目標値。RLO。
	モデルシステム	経済産業省の信頼性ガイドラインやIPAの重要インフラ情報システム信頼性研究会報告書を参考に非機能要求項目を定義したシステムの例。以下の3つの例を提供している。 ・社会的影響が極めて大きいシステム ・社会的影響が限定される大きいシステム ・社会的影響が殆ど無いシステム
	モデルシステムシート	モデルシステム毎の特徴を示す代表的な非機能要求をまとめたもの。グレード表に同梱している。
【や】	床荷重	床の平方メートル当りに設置可能な重量。値が大きいほど沢山の機材を集中的に設置できる可能性がある。通常のオフィスでは、300Kg/㎡程度だが、データセンターなどでは、1,000Kg/㎡以上に達する場合もある。
	予兆監視	システムに致命的な障害が発生する前に、機器の軽微なエラーやリソース使用状況などを監視し、トラブルが起こりそうな兆候を感知すること。予防保守などの実施が可能となる。 (関連用語) → 予防保守
	予備機	障害が発生したサーバや端末のための交換用機器のこと。
	予防保守	主に消耗品に関して、故障が発生する前に決められたタイミングにて交換を実施すること。使用期間に基づいて実施する方法と、予兆監視の結果に基づいて実施する方法がある。 (関連用語) → 予兆監視
【ら】	ラックマウント用機材	19インチラックなどに搭載することを前提に設計された機材。
	リソース	CPU/メモリ/ストレージなど、情報システムを満足に作動させるために必要な資源の総称。
	リソース監視	監視対象のリソースの過不足に関する状態を確認する監視方式。

【A-Z】

用語	説明
リモート監視	監視対象が存在する場所とは異なる場所へ監視結果を通知する監視環境の実現方式。
リモート操作	情報システムに対する運用作業あるいは保守作業を情報システムが存在する場所とは異なる場所から実行する運用環境の実現方式。
レスポンス	システム等にリクエスト（要求）を送信してから最初の応答（結果）が返ってくるまでの時間。バッチの場合はターンアラウンドタイム（最初の結果が返ってくるまでの時間）と同じ。 （関連用語） → ターンアラウンド（タイム）
レスポンス順守率	システムが目標とするレスポンスを達成させることができる割合（業務処理の中で、全トランザクションが目標として決めたレスポンスをどれだけ達成できるか）。 レスポンス順守率＝（定義した目標値を満たしたトランザクション件数）／（全トランザクション件数）
レベル	メトリクスに対して通常取りうる値を0から5までの6段階に整理したもの。ただし、レベルの段階が6つに満たない場合は左詰めとなっている。
レベル値	メトリクス毎に具体的な実現レベルを定義したもの。0から5のいずれかの数値とその数値が示す内容の説明から構成される。
漏電対策	漏電によるシステムへの被害を防ぐための対策。感知対策、遮断対策などがある。 （関連用語） → 遮断対策
ログローテート	ログファイルの肥大化を防ぐため、一定期間や一定サイズでログファイルを切り替えたり、過去ログを削除したりする機能のこと。
ローリングアップグレード	クラスタ構成やデュアル構成のシステムにおいて、系切替や縮退運用を活用してノード毎に順にパッチ適用を行うことで、システムの運用を停止せずにパッチ適用を実現する方法のこと。
BtoB (Business to Business)	企業間取引のこと。取引相手は予め契約した企業であり固定的なことが多い。B2B。
BtoC (Business to Consumer)	ネットワークを介した企業と消費者間の取引形態。一般に消費者は不特定多数となることが多く、システムの需要予測が難しい側面がある。B2C。
CO ₂ 排出量	サービスを提供するためのシステムによって排出されるCO2の量。サービス提供中の運転によるエネルギー消費だけではなく、機材の生産・廃棄を含めたライフサイクル全体で排出量を捉える必要がある。温室効果ガス抑制を謳った京都議定書での排出量取引や炭素税などでの削減動機付けが検討されている。
CPU利用率	システム上でOSやアプリケーションが処理をする際にCPUを使用している割合。通常は単位時間内の平均利用率を示す。 CPU利用率＝（単位時間中でCPUが使われた時間）／（単位時間）
CSIRT (Computer Security Incident Response Team)	セキュリティインシデントの対応を行う組織のこと。インシデントを早期発見し、早期対応で被害を最小化することを目的とする。脆弱性情報の収集や脅威の分析、インシデント対応マニュアルの整備、インシデント発生時の緊急対応を行うほか、セキュリティ教育等も実施する。
CSR (Corporate Social Responsibility)	企業の社会的責任。具体的には、利害関係者に対する説明責任、法令順守、および、企業統治などの活動を指す。自身を自発的に律する活動であることが、公告・宣伝活動などとは基本的に異なる。企業が永続的に存続・発展できるための社会的信用を醸成することを目的としていることが多い。
dB (decibel)	本来のデシベルは無次元の単位を表すが、本書では慣用的に騒音の音圧レベルの単位として用いている（正確には、dB SPL）。対数表現を採っており、6dBで約2倍、10dBで約3倍の音圧を意味し、例えば、60dBは50dBの約3倍の音圧を意味する。
DB診断 (DataBase診断)	診断対象のデータベースに対して、システム内部および外部からの攻撃を想定し、脆弱な設定が存在しないか等を分析すること。
DR (Disaster Recovery)	災害や故障など予期せぬ事象が発生し、システムに甚大な影響が及んだ際に、業務を復旧するための手段あるいは計画のこと。
DRサイト	大規模災害で通常運用しているシステムの復旧が不可能な場合に、代替できるシステムを設置したサイト。
IHV (Independent Hardware Vendor)	特定のハードウェアメーカーの傘下に入っていない、オリジナルのハードウェアを製造・販売しているハードウェア企業のこと。

用語	説明
ISV (Independent Software Vendor)	特定のソフトウェアメーカーの傘下に入っていない、オリジナルのソフトウェアを製造・販売しているソフトウェア企業のこと。
MTBF (Mean Time Between Failure)	システムが故障してから次の故障までの平均的な間隔（時間）のこと。平均故障間隔。稼働時間（運用時間）の合計値を、発生した故障回数で割った値で表わされる。
MTTR (Mean Time To Repair / Mean Time To Recover)	システムに故障が発生してから復旧するまでの平均的な時間のこと。システムの復旧時間の合計値を、発生した故障回数で割った値で表わされる。
RAID (Redundant Arrays of Independent(Inexpensive) Disks)	複数のハードディスクを組み合わせ、信頼性の向上、高速化を可能とする技術。ミラーリングを行うRAID1、誤り訂正符号を複数のディスクに分散させて信頼性を向上させるRAID5などがある。
RLO (Recovery Level Objective)	業務停止を伴う障害が発生した際、どこまで復旧するかレベル（システムのための復旧か、すぐにも業務が再開できる状態か）の目標値。目標復旧レベル。
RoHS指令 (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment)	欧州連合(EC)が定めた電気電子機器に含まれる特定有害物質の使用制限に関する指令。有害物質を含んだ電気電子機器の処分による環境への影響を考慮したもの。対象六物質(鉛、水銀、カドミウム、六価クロム、ポリ臭化ビフェニール、ポリ臭化ジフェニルエーテル)の最大濃度許容値等を定めている。欧州連合加盟国域内で上市される電気電子機器に適用される。
RoSPA (The Royal Society for the Prevention of Accidents)	英国王立災害防止協会。労働災害防止のための騒音基準などを定めている。
RPO (Recovery Point Objective)	業務停止を伴う障害が発生した際、バックアップしたデータなどからシステムをどの時点まで復旧するかを定める目標値。目標復旧地点。
RT0 (Recovery Time Objective)	業務停止を伴う障害が発生した際、RPOおよびRLOで設定した目標値に対して復旧するまでに要する目標時間。目標復旧時間。実際に復旧のために要した時間の合計値は、平均復旧時間（MTTR）として稼働率の計算に利用する。 （関連用語） → RPO、RLO、MTTR
Sorry動作	システムに高負荷が発生したときに、単に無応答になるのではなく、利用者に対して「現在混みあっています」などの現状報告や代替手段の案内を提供すること。設計されていない場合は無応答になることが多い。
SPOF (Single Point of Failure)	該当箇所にて故障が発生した場合、システム停止となってしまうコンポーネント。単一障害点。
UL60950	世界的に著名なIT機器に関する製品安全規格。米国の独立系の安全規格開発機関、試験・認証機関であるUnderwriters Laboratories Inc.（略称：UL）が策定。
VCCI (Voluntary Control Council for Interference by Information Technology Equipment)	パーソナルコンピュータ、ファクシミリ等の情報技術装置によるラジオ、テレビジョン等の受信機への電波障害問題と対策を講ずるための国内業界の自主規制団体「情報処理装置等電波障害自主規制協議会」の略称。自主規制には、VCCI クラスAまたはクラスBの2つがあり、家庭環境向けのクラスBの方がより厳しい基準となっている。
WAF (Web Application Firewall)	WebサーバやWebアプリケーションの脆弱性を狙った攻撃に対し、それらに受け渡されるデータを検知し、遮断するためのファイアウォール。
Web診断	Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のこと。

5 付録

5.1 非機能要求に関する他活動との関係について

非機能要求グレードの他にも「非機能要求」に関する標準やガイドラインがある。非機能要求グレードと他活動との差を示し非機能要求グレードの位置づけを明らかにするため、他ガイドラインとの関係を主たる想定利用工程で表すと以下のような図式となる。

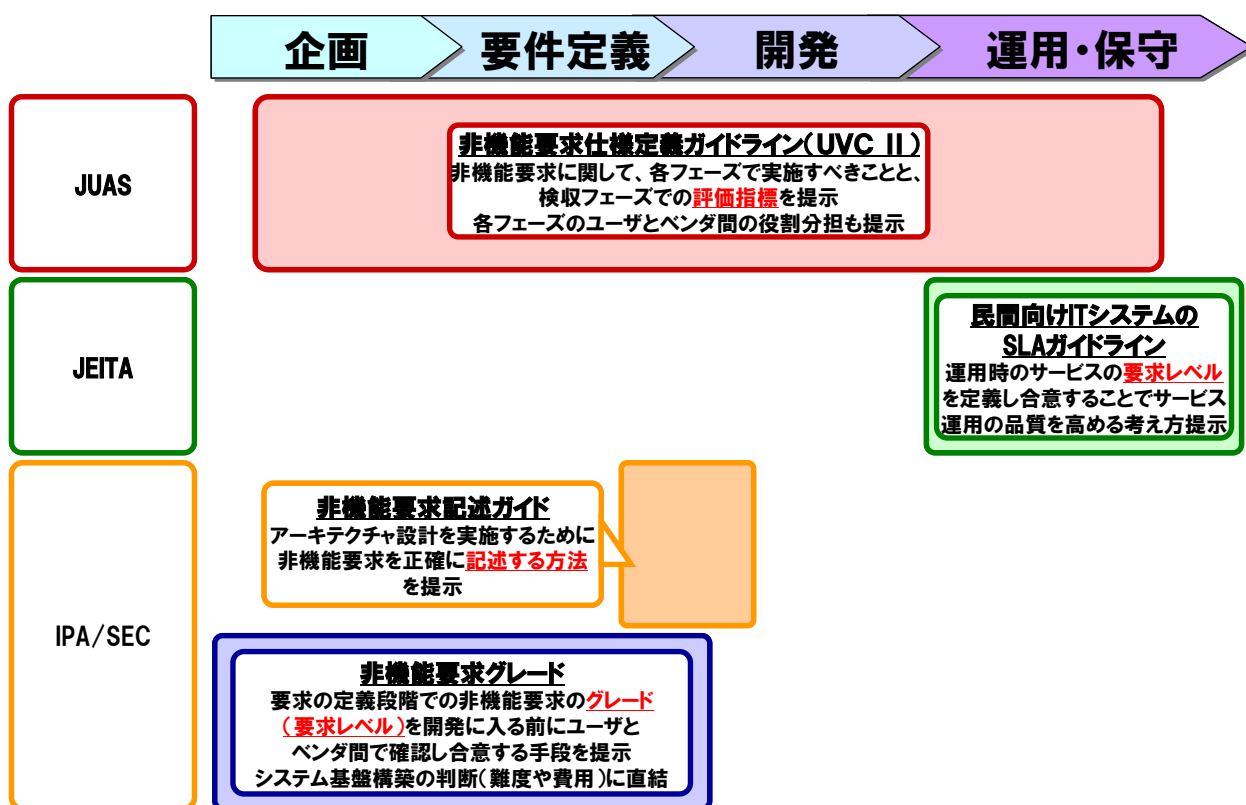


図 5.1.1 想定利用工程と各種標準活動

非機能要求グレードは、主として上流工程における要求項目とその要求レベルをユーザ/ベンダ間で確認し合意することを狙っており、別の狙いを持った他ガイドラインと共に利用することが考えられる。以下では他ガイドラインとの関係を示す。

5.1.1 JUAS「非機能要求仕様定義ガイドライン 2008」との関係

「非機能要求仕様定義ガイドライン 2008 (以下、UVC II)」は、社団法人 日本情報システム・ユーザー協会 (JUAS) が策定したガイドラインであり、システム発注者の視点で、システム全体の非機能要求に関して、発注者がシステムを検収する際に検証すべき非機能要求項目の整理を行っている。具体的には、上流工程から下流工程の各段階での要求定義の方法、特に測定可能な要求定義項目の定め方を示し、それらの検証ポイントを示している点に

特徴がある。また、取り扱う非機能要求項目を幅広く、機能性、信頼性、使用性、効率性、保守性、移植性、障害抑制性、効果性、運用性、技術要件の 10 分類としている。

UVC II と非機能要求グレードには、取り扱う非機能要求項目の範囲において差がある。非機能要求グレードでは、システム基盤を判断するための非機能要求を検討範囲とすることで、要求項目毎にシステム基盤の構築難度毎の要求レベルを示している。このため、UVC II で着目している分類の中でも、機能性、使用性、移植性など、システム基盤の判断に直接関係のない項目については大部分をスコープ外としている点が異なる。

両者を利用する場合、システム全体の非機能要求を上流から検収に至るまで定義していくことには UVC II を用いることができる。ただし特に上流において具体的なシステム基盤が備えるべき非機能要求を確認・合意する際には「非機能要求グレード」を用いるとより効果的である。

5.1.2 JEITA「民間向け IT システムの SLA ガイドライン」との関係

社団法人 電子情報技術産業協会（JEITA）によって既に第三版まで改訂されている「民間向け IT システムの SLA ガイドライン」は、情報システムによって提供される IT サービス品質を評価する指標としての SLA および SLA を用いた IT サービスの運用レベルの向上を目指す考え方を示している。また、2009 年 3 月発行の「SLA 適用領域拡大に関する調査報告書」ではシステム開発の SLA および開発と運用をつなぐ連携指標を示している。

非機能要求グレードは主に開発時の判断としての要求レベルを示しており、運用時のサービスレベルを示す SLA とは利用タイミングが異なる。両者を利用する場合、開発契約や運用契約などの場面の違いに合わせそれぞれのタイミングで利用することが考えられる。

5.1.3 IPA/SEC「非機能要求記述ガイド」との関係

情報処理推進機構ソフトウェア・エンジニアリング・センター（IPA/SEC）によって 2008 年 7 月にまとめられた「非機能要求記述ガイド」では、システムのアーキテクチャ設計のために正確で十分な非機能要求を効率的、かつ網羅的に記述する方法を提示するために、記述項目をテンプレート化するなど記述ルールを定めている。

非機能要求を定義する者は非機能要求グレードを用いて、まず企画・要件定義の時点での要求レベルの確認を行い、「非機能要求記述ガイド」を参考に要件定義をより詳細に記述するといった利用が可能である。

5.2 他活動との関係について

非機能要求グレードは、策定にあたって、「考え方を踏襲している」、「引用している」、「用語を合わせている」など標準規格を参考に行っていることがある。また、非機能要求グレードは、単独で非機能に関する要求についてユーザとベンダ間で合意できるように考慮されているが、他に順守すべき規程等が存在する場合、それらの規程等と合わせて検討する必要がある。

以下の項ではそれら他の標準との関係について説明する。

5.2.1 ISO/IEC 9126-1:2001 との関係

非機能要求に関係する代表的な標準として、「ISO/IEC 9126-1:2001 (JIS X0129-1:2003)¹⁾」(以下 ISO/IEC 9126) がある。ISO/IEC 9126 は、ソフトウェアを対象として外部品質と内部品質の両面から品質特性を定義している国際標準規格である。

システム基盤の非機能要求を対象としている非機能要求グレードとは一概に比較できないが、用語は可能な範囲で ISO/IEC 9126 を参考に行っている。ソフトウェアの品質特性を定義している ISO/IEC 9126 をシステム基盤に対する品質特性を定義しているものと仮に解釈して比較した場合、非機能要求グレードの各大項目との対応関係は表 5.2.1.1 のようになる。

この表の対応関係を見ると、ISO/IEC 9126 の品質副特性と、非機能要求グレードの大項目では対応が無い部分がある。対応関係がない理由は、1.3 節で示すスコープのとおり、非機能要求グレードがシステム基盤に対する発注者の要求を「見える化」することを目的としているために主にソフトウェアだけから作られるアプリケーションの品質を示す部分については、検討対象から外しているためである。例えば、「使用性」のようにソフトウェアからなるアプリケーションの性質としては存在するが、システム基盤の性質としては対象外になっている。

¹⁾ 2009 年 12 月現在、ISO/IEC 9126 の後継の規格となる SQuaRE (Software Product Quality Requirements and Evaluation) と呼ばれる ISO/IEC 25000 シリーズが整備中である。全体のガイドである ISO/IEC 25000:2005 の他、ISO/IEC 25030:2007 Quality Requirements などが発行されている。

表 5.2.1.1 ISO/IEC 9126 と非機能要求グレードの対応関係

特性	定義	品質副特性	定義	対応する大項目
機能性	ソフトウェアが、指定された条件の下で利用されるときに、明示的及び暗示的の必要性に合致する機能を提供するソフトウェアの能力	合目的性	指定された作業及び利用者の具体目標に対して適切な機能の集合を提供するソフトウェア製品の能力	—
		正確性	必要とされる精度で、正しい結果若しくは正しい効果、又は同意できる結果若しくは同意できる効果をもたらすソフトウェア製品の能力	—
		相互運用性	一つ以上の指定されたシステムと相互作用するソフトウェア製品の能力	—
		セキュリティ	許可されていない人又はシステムが情報又はデータを読んだり、修正したりすることができないように、及び許可された人又はシステムが情報又はデータへのアクセスを拒否されないように、情報又はデータを保護するソフトウェア製品の能力	セキュリティ
		機能性標準適合性	機能性に関連する規格、規約又は法律上及び類似の法規上の規則を遵守するソフトウェア製品の能力	セキュリティ、システム環境・エコロジー
信頼性	指定された条件下で利用するとき、指定された達成水準を維持するソフトウェア製品の能力	成熟性	ソフトウェアに潜在する障害の結果として生じる故障を回避するソフトウェア製品の能力	可用性
		障害許容性	ソフトウェアの障害部分を実行した場合、又は仕様化されたインタフェース条件に違反が発生した場合に、指定された達成水準を維持するソフトウェア製品の能力	可用性
		回復性	故障時に、指定された達成水準を再確立し、直接に影響を受けたデータを回復するソフトウェア製品の能力	可用性、運用・保守性
		信頼性標準適合性	信頼性に関連する規格、規約又は規則を遵守するソフトウェア製品の能力	システム環境・エコロジー
使用性	指定された条件の下で利用するとき、理解、習得、利用でき、利用者にとって魅力的であるソフトウェア製品の能力	理解性	ソフトウェアが特定の作業に特定の利用条件で適用できるかどうか、及びどのように利用できるかを利用者が理解できるソフトウェア製品の能力	—
		習得性	ソフトウェアの適用を利用者が習得できるソフトウェア製品の能力	運用・保守性
		運用性	利用者がソフトウェアの運用及び運用管理を行うことができるソフトウェア製品の能力	運用・保守性
		魅力性	利用者にとって魅力的であるためのソフトウェア製品の能力	—
		使用性標準適合性	使用性に関連する規格、規約、スタイルガイドまたは規則を遵守するソフトウェア製品の能力	システム環境・エコロジー
効率性	明示的な条件の下で、使用する資源の量に対比して適切な性能を提供するソフトウェア製品の能力	時間効率性	明示的な条件の下で、ソフトウェアの機能を実行する際の、適切な応答時間、処理時間及び処理能力を提供するソフトウェア製品の能力	性能・拡張性
		資源効率性	明示的な条件の下で、ソフトウェアの機能を実行する際の、資源の量及び資源の種類を適切に使用するソフトウェア製品の能力	性能・拡張性
		効率性標準適合性	効率性に関連する規格または規約を遵守するソフトウェア製品の能力	性能・拡張性、システム環境・エコロジー
保守性	修正のしやすさに関するソフトウェア製品の能力	解析性	ソフトウェアにある欠陥の診断または故障原因の追及、及びソフトウェアの修正箇所の識別を行うためのソフトウェア製品の能力	運用・保守性
		変更性	指定された修正を行うことができるソフトウェア製品の能力	—
		安定性	ソフトウェアの修正による、予期せぬ影響を避けるソフトウェア製品の能力	—
		試験性	修正したソフトウェアの妥当性確認ができるソフトウェア製品の能力	—
		保守性標準適合性	保守性に関連する規格又は規約を遵守するソフトウェア製品の能力	運用・保守性、システム環境・エコロジー
移植性	ある環境から他の環境に移すためのソフトウェア製品の能力	環境適用性	ソフトウェアにあらかじめ用意された以外の付加的な作業または手段なしに、指定された異なる環境にソフトウェアを適応させるためのソフトウェア製品の能力	移行性
		設置性	指定された環境に設置するためのソフトウェア製品の能力	システム環境・エコロジー
		共存性	共通の資源を共有する共通の環境の中で、他の独立したソフトウェアと共存するためのソフトウェア製品の能力	移行性
		置換性	同じ環境で、同じ目的のために、他の指定されたソフトウェア製品から置き換えて使用することができるソフトウェア製品の能力	移行性
		移植性標準適合性	移植性に関連する規格又は規約を遵守するソフトウェア製品の能力	システム環境・エコロジー

5.2.2 共通フレーム 2007 との関係

共通フレーム 2007 は、システム構築に関わる作業項目の共通の枠組みを受発注者に提供するものである。システムの構想から廃棄までに必要となる作業項目や役割について、作業工程や開発モデルおよび開発技法/ツールに依存せず、産業界の総意として包括的に規定したものである。また、ソフトウェア・ライフサイクル・プロセス（SLCP-JCF2007）の国際規格 ISO/IEC 12207:2007（JIS X 0160）を基盤として、ソフトウェアを中心としたシステム関連作業を含み、特に上流工程などで日本独自に強化、拡張されている。

非機能要求グレードでは、この共通フレーム 2007 を業界のシステム構築作業やプロセスの標準規格として捉え、規定されている項目や役割分担などを参考にした。

5.2.3 情報システムの信頼性向上に関するガイドラインとの関係

情報システムの信頼性向上に関するガイドライン（信頼性ガイドライン）とは、情報システム障害の社会に与える影響が深刻化してきたことを受けて、経済産業省が 2006 年に第 1 版、2009 年 3 月に第 2 版を策定したガイドラインである。その策定目的を背景に、非機能要求の中でも特に信頼性・安全性に主眼を置き、その水準向上を目的としている。ガイドラインでは信頼性向上のために受発注者双方の開発時、運用時、障害発生時の実施項目、あるいは、技術的な留意事項が種別毎に示されている。

非機能要求グレードでは、この信頼性ガイドラインの関連施策である「重要インフラ情報システム信頼性研究会」の示すシステムプロファイルの名称を使用して 3 つのモデルシステムを再定義して例示している。また、非機能要求グレード自体は同省の信頼性向上施策の 1 テーマである要件定義の「共通認識支援ツール」として同省へ協力しながら検討を進めており、信頼性ガイドラインを中心とする他施策の中に位置付けられている。

5.2.4 ISO/IEC 15408 (Common Criteria) との関係

ISO/IEC 15408:1999 とは、情報システムやそれを構成する機器・ソフトウェアのセキュリティの評価基準を定めた国際標準規格である。3 部構成となっており、ISO/IEC 15408-1:2005、ISO/IEC 15408-2:2008、ISO/IEC 15408-3:2008 の 3 つの規格が発行されている。非機能要求グレードにおいても、システムのセキュリティに関する基本的な概念や用語などについては、ISO/IEC 15408 の内容を踏襲している。

ISO/IEC 15408 は、欧米 6 カ国による CC プロジェクトで開発された Common Criteria と呼ばれるセキュリティ評価基準を国際標準化したものであり、ISO/IEC 15408 に基づく「IT セキュリティ評価及び認証制度」が国際間（日本を含む）で広く運用されている。日本国内でも、主に政府機関のシステムの調達にて ISO/IEC 15408 に基づく評価・認証制度が活用されている²。以下にその例を示す。

² 「ISO/IEC 15408 を活用した調達のガイドブック（経済産業省 商務情報政策局 情報セキュリティ政策室）」を参照のこと。

① システムの特定の構成要素に対して用いられるケース

システムを構成するセキュリティ製品に対し、ISO/IEC 15408 に基づく評価・認証の取得が要求事項として提示されるケースがある。特に IC カード、暗号製品、ファイアウォールなど、高度なセキュリティが求められるシステム構成要素に適用される。

② ISO/IEC 15408 に基づくセキュリティ設計仕様書が求められるケース

ISO/IEC 15408 では ST (Security Target) と呼ばれる「セキュリティ設計仕様書」が定義されており、開発対象のシステムに高いセキュリティが要求される場合に、ISO/IEC 15408 に基づく「セキュリティ設計仕様書」の作成および第三者評価機関による内容の妥当性の評価が求められる場合がある。

これらがシステムの要求事項として挙げられた場合にシステムの開発コストに影響するため、あらかじめ対応の要否を確認しておく必要がある。

5.2.5 ISO/IEC 27000 シリーズとの関係

ISO/IEC 27000 シリーズとは、情報セキュリティを確保・維持するため、組織内で実施すべき取り組みを体系化・系統化した ISMS (情報セキュリティマネジメントシステム) に関する国際標準規格である。

2009 年 12 月末時点では、ISO/IEC 27001:2005 (要求事項) および ISO/IEC 27002:2005 (実践のための規範) などが発行されている³。また日本国内では、ISO/IEC 27001 への適合性の評価・認定を行う「ISMS 適合性評価制度」が運用されており、企業、組織などで広く普及している。

ISMS は、システムのみならずこれを運用する組織を対象に、技術的、物理的、人的、組織的の各管理策を定め、経営層を頂点に組織的に実施するものである。非機能要求グレードではシステムの要求導出をスコープとしているが、システムを利用、運用する側の物理的、人的、組織的なセキュリティ要求を導出する際には、ISO/IEC 27002 に具体的な管理策がベストプラクティスとして示されており、これを参考にすることができる。

また、ISMS 認証を取得済み（もしくは取得予定）の組織内で運用するシステムのセキュリティ要求を導出する際には、ISMS で策定した技術的な管理策との整合を図る必要がある。これには、主に項目一覧の中項目「アクセス・利用制限」、「不正追跡・監視」、「ネットワーク対策」などが該当する。

³ 2009 年 12 月末現在、ISO/IEC 27000 シリーズは整備中であり、上記の他、ISO/IEC 27005:2008 (情報セキュリティリスクマネジメント)、ISO/IEC 27006:2007 (監査及び認証機関の要求事項) 等が発行されている。

5.2.6 政府機関の情報セキュリティ対策のための統一基準との関係

政府機関の情報セキュリティ対策のための統一基準（政府統一基準）とは、国内政府機関（各府省庁）の情報セキュリティ対策の基準を示したものである。政府機関のシステムを構築する際には政府統一基準に従うことが義務付けられており、セキュリティ要求の導出された結果が政府統一基準に準拠することを十分に確認する必要がある。

政府統一基準では、実施すべきセキュリティ対策を「基本」（必須の対策）、「強化」（任意で実施する対策）に分類しており、必ずしも全てのセキュリティ対策を必須として規定していない。そのため、政府機関向けシステムに非機能要求グレードを用いる際には、政府統一基準で必須とするセキュリティ対策についてはそれに従い、必須以外のセキュリティ対策については、非機能要求グレードを参考に要求を導出するなどの使い方ができる。

なお、政府統一基準で定める情報セキュリティ対策では、広くセキュリティを捉えており、システムの災害・障害に対する「可用性」や、これを維持するための「運用・保守性」に関する対策も含んでいる。「可用性」、「運用・保守性」の要求を検討する際にも、政府統一基準との整合を十分に確認する必要がある。

5.2.7 金融機関等コンピュータシステムの安全対策基準との関係

金融機関等コンピュータシステムの安全対策基準（FISC 安全対策基準）とは、金融情報システムセンター（FISC）が定めた、国内金融機関におけるセキュリティ対策の基準である。通常、金融機関のシステム構築においては FISC 安全対策基準への準拠が調達の条件となるため、セキュリティ要求を導出する際には、その結果が FISC 安全対策基準に準拠することを十分に確認する必要がある。

FISC 安全対策基準においても、政府統一基準と同様、実施すべきセキュリティ対策を、必須の項目と任意の項目の 2 種類でレベル付けしており、金融機関システムに非機能要求グレードを用いる際には、FISC 安全対策基準で必須とするセキュリティ対策についてはそれに従い、必須以外のセキュリティ対策については、非機能要求グレードを参考に要求を導出するなどの使い方ができる。

なお、FISC 安全対策基準で定める対策は、金融システムの性質上、システムの災害・障害に対する「可用性」や、運用施設など「システム環境・エコロジー」に関する対策も多く含んでおり、「可用性」、「システム環境・エコロジー」の要求を検討する際にも、FISC 安全対策基準との整合を十分に確認する必要がある。

5.2.8 Payment Card Industry Data Security Standard との関係

Payment Card Industry Data Security Standard (PCI DSS) とは、クレジット業界で定めた国際的なセキュリティ基準であり、クレジットカード加盟店および決済代行事業者が扱うクレジットカード情報に対するセキュリティを対象としている。

クレジットカード加盟店などのクレジットカード情報を扱うシステムにおいては、PCI DSS への準拠が必要となるため、これに該当するシステムのセキュリティ要求を導出するには、その結果が PCI DSS に準拠することを十分に確認する必要がある。

PCI DSS が適用されるシステムに非機能要求グレードを用いる際には、まずは PCI DSS で示されている要求についてそれに従い、PCI DSS で要求が明確に示されていない項目については、非機能要求グレードを参考に要求を導出するなどの使い方ができる。

5.3 参考文献

- [1] 独立行政法人 情報処理推進機構ソフトウェアエンジニアリングセンター(IPA/SEC), 『共通フレーム 2007 ～経営者、業務部門が参画するシステム開発および取引のために～』, オーム社, 2007 年 10 月 1 日
- [2] 独立行政法人 情報処理推進機構ソフトウェアエンジニアリングセンター(IPA/SEC), 『経営者が参画する要求品質の確保 ～超上流から攻める IT 化の勘どころ～ 第 2 版』, オーム社, 2006 年 5 月 25 日
- [3] 経済産業省 ソフトウェア開発力強化推進タスクフォース 要求工学・設計開発技術研究部会 非機能要求とアーキテクチャ WG, 『非機能要求記述ガイド』, <https://www.ipa.go.jp/files/000004469.pdf>, 2008 年 7 月
- [4] 社団法人 日本情報システム・ユーザー協会(JUAS), 『非機能要求仕様定義ガイドライン 2008』, 2008 年 7 月
- [5] 社団法人 電子情報技術産業協会(JEITA) ソリューションサービス事業委員会, 『民間向け IT システムの SLA ガイドライン 第三版』, 日経 BP 社, 2006 年 10 月 2 日
- [6] 社団法人 電子情報技術産業協会(JEITA) ソリューションサービス事業委員会, 『SLA 適用領域の拡大に関する調査報告書』, 社団法人 電子情報技術産業協会, 2009 年 3 月
- [7] 経済産業省, 『情報システムの信頼性向上に関するガイドライン』, 2006 年 6 月 15 日
- [8] 経済産業省, 『情報システムの信頼性向上に関するガイドライン 第 2 版』, 2009 年 3 月 24 日
- [9] 経済産業省 商務情報政策局 情報セキュリティ政策室, 『ISO/IEC 15408 を活用した調達のガイドブック』, http://www.meti.go.jp/policy/netsecurity/docs/cc/CCguide_ver2_0.pdf, 2004 年 8 月 11 日
- [10] 内閣官房情報セキュリティセンター(NISC), 『政府機関の情報セキュリティ対策のための統一基準』, <http://www.nisc.go.jp/active/general/kijun01.html>, 2009 年 2 月 3 日
- [11] 金融情報システムセンター(FISC), 『金融機関等コンピュータシステムの安全対策基準・解説書(第 7 版)』, 金融情報システムセンター(FISC), 2006 年 3 月
- [12] ISO/IEC 9126-1:2001(Software engineering -- Product quality -- Part 1: Quality model), 2001 年
- [13] ISO/IEC 15408-1:2005(Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model), 2005 年
- [14] ISO/IEC 15408-2:2005(Information technology -- Security techniques --

- Evaluation criteria for IT security -- Part 2: Security functional requirements) ,
2005 年
- [15] ISO/IEC 15408-3:2005(Information technology -- Security techniques --
Evaluation criteria for IT security -- Part 3: Security assurance requirements) ,
2005 年
- [16] ISO/IEC 27001:2005(Information security management systems - Requirements),
2005 年
- [17] ISO/IEC 27002:2005(Code of practice for information security management), 2005
年
- [18] PCI Security Standards Council, 『Payment Card Industry(PCI) データセキュリ
ティ基準 - 要件とセキュリティ評価手順 バージョン 1.2』 ,
https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf,
2008 年 10 月
- [19] 独立行政法人 情報処理推進機構ソフトウェアエンジニアリングセンター(IPA/SEC),
重要インフラ情報システム信頼性研究会報告書,
<http://sec.ipa.go.jp/reports/20090409.html>, 2009 年 4 月
- [20] 経済産業省, 非機能要求グレード「ユーザビュー検討委員会」報告書,
http://www.meti.go.jp/policy/it_policy/softseibi/hikinou_grade.pdf, 2009 年 6 月