

# 非功能性要求等级使用向导 《解说篇》

2013 年 3 月

独立行政法人 信息处理推进机构

技术部 软件工程中心

## 使用条件

1. 本资料是独立行政法人 信息处理推进机构拥有著作权作品的衍生作品，本资料著作权由株式会社 恩梯梯数据所有。使用本资料需遵循以下条件。
2. 本资料受日本著作法及其它国际性著作权保护相关规定的保护。本资料的使用者在使用本资料的全部或者一部分时，除了遵守第3项以外，没有独立行政法人 信息处理推进机构和株式会社 恩梯梯数据的许可，不论是盈利目的或者非盈利目的，禁止擅自更改、公众发送、销售、出版、翻译/改编等活动。
3. 独立行政法人 信息处理推进机构和株式会社 恩梯梯数据，在本资料的使用者注明以下著作权表示的条件下，允许①及②的行为。

著作权表示：Copyright © 2010 IPA

Revised 2013 NTT DATA Corporation

  - ①复制本资料的全部或部分。
  - ②使用者遵守本页记载的使用条件为前提条件，可无偿再发本资料的复印件。
4. 独立行政法人 信息处理推进机构和株式会社 恩梯梯数据，不能完全保证本资料与第三方的著作权、特许权、实用新发明权等知识产权不相抵触。并且，即使本资料的内容有错误也不负任何责任。
5. 独立行政法人 信息处理推进机构和株式会社 恩梯梯数据，除了本页记载的承诺内容以外，对于独立行政法人 信息处理推进机构、株式会社 恩梯梯数据或第三方的著作权、特许权、实用新发明权等基于知识产权的任何权利，都不予承诺。
6. 独立行政法人 信息处理推进机构和株式会社 恩梯梯数据，不对利用本资料开发系统、所开发系统的使用及因该系统不能使用等而产生的损害承担任何责任。
7. 将本资料带到海外及提供给非居住者时，需在确认《外汇及外国贸易法》的规定及美国出口管理规定等外国的出口相关法规后，办理必要手续。
8. 本使用条件的诠释遵循日本国法律，就本资料的使用发生法律纠纷时，以东京地方法院为唯一的协定管辖法院。

非功能性要求等级使用向导《解说篇》

非功能性要求等级使用向导，如下图所示，由《使用篇》和《解说篇》构成。

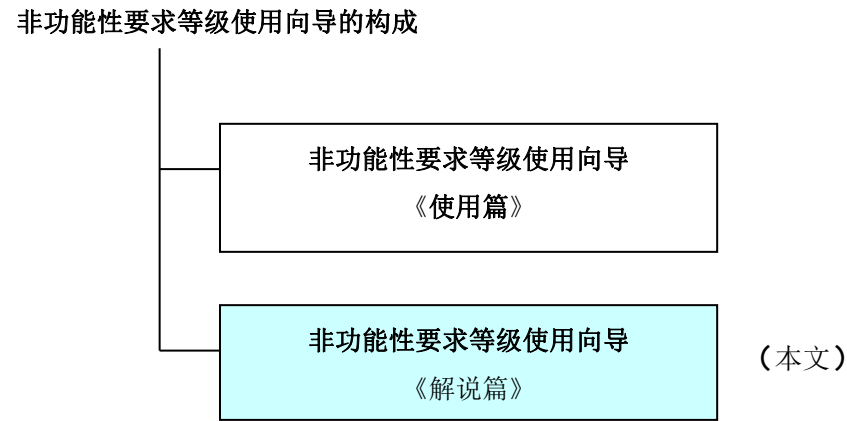


图 . 非功能性要求等级使用向导《解说篇》的定位

本文是以解释说明可以预测系统基础的发包方要求的非功能性要求等级的作成背景、工具详情等为目的。

关于非功能性要求等级的使用方法，请参照《使用篇》。

“非功能性要求等级”是，非功能性要求等级使用向导及以下 3 个工具表的总称。

- “关于系统基础的非功能性要求等级表（以下简称等级表）”
- “关于系统基础的非功能性项目一览表（以下简称项目一览）”
- “关于系统基础的非功能性要求树形图（以下简称树形图）”

本文的主要阅读对象

本文的主要阅读对象是针对企业的业务系统，信息系统的开发，关系到在需求定义等情况下提示、提案及决定非功能性要求的发包方与承包方的负责人。并且，在以后本文中的发包方统一称为用户、承包方的统一称为供应商。

本文的构成

本向导如下图所示。

表. 非功能性要求等级使用向导《解说篇》的构成

章编号	章題	概要
1 章	前言	关于非功能性要求等级制定的背景及范围等的说明。
2 章	非功能性要求等级的详细说明	关于非功能性要求等级的做法及各个大项的说明。
3 章	FAQ	关于非功能性要求等级经常被问到的问题及回答的说明。
4 章	用语集	关于非功能性要求等级使用的词语说明。
5 章	附录	与其他标准相关联等、补充信息的说明。

## 目录

1 前言	1
1.1 非功能性要求等级制定的背景及目的	1
1.2 非功能性要求的问题及非功能性要求等级的解决方法	4
1.3 非功能性要求等级的范围	5
1.3.1 非功能性要求的定义及与系统基础的关系	5
1.3.2 范围项目	5
1.3.3 关于范围以外的项目	7
1.4 非功能性要求等级的概要	8
1.4.1 非功能性要求等级的基本理念	8
1.4.2 非功能性要求等级的构成要素・概要	9
2 非功能性要求等级的详细说明	13
2.1 非功能性要求等级的详细说明	13
2.1.1 等级表	13
2.1.2 项目一览	17
2.1.3 树形图	19
2.2 各大项的概要及注意事项	20
2.2.1 可用性	20
2.2.2 性能・扩展性	22
2.2.3 运用・维护性	23
2.2.4 可转移性	24
2.2.5 安全措施	25
2.2.6 系统环境・低碳环保	27
3 FAQ	28
4 用语集	33
5 附录	40
5.1 与有关非功能性要求其他活动的关系	40
5.1.1 与 JUS “非功能性要求做法定义指导方针 2008” 的关系	40
5.1.2 与 JEITA “面向民众 IT 系统的 SLA 指导方针” 的关系	41
5.1.3 与 IPA/SEC “非功能性要求记述向导” 的关系	41

5.2 与其他活动的关系	42
5.2.1 与 ISO/IEC 9126-1:2001 的关系	42
5.2.2 与标准框架 2007 的关系	44
5.2.3 与关于增强信息系统的信赖性指导方针的关系	44
5.2.4 与 ISO/IEC 15408(Common Criteria)的关系	44
5.2.5 与 ISO/IEC 27000 系列的关系	45
5.2.6 与政府机关信息安全措施对策的统一标准的关系	45
5.2.7 与金融机关等计算机系统安全对策标准的关系	46
5.2.8 与 Payment Card Industry Data Security Standard 的关系	46
5.3 参考文献	47

# 1 前言

## 1.1 非功能性要求等级制定的背景及目的

最近，信息系统已成为社会活动及企业活动不可或缺一部分。图 1.1.1 显示了信息系统的历史性变迁。现在，如果没有 IT 就不能形成商务贸易，另外，信息系统的使用者也不仅限一个公司内部，同时已扩展到公司外及一般消费者当中等。伴随着信息系统社会基础化，能提供稳定的可靠的信息系统的服务，与以前相比显得尤为重要。信息系统的构成要素，也就是被应用的技术与成品已成为更加开放化、网络化的大规模并且复杂的东西。因此实现信息系统已不再是单纯的业务 IT 化,更为重要的是把复杂的构成要素恰当地结合并提供稳定的服务。

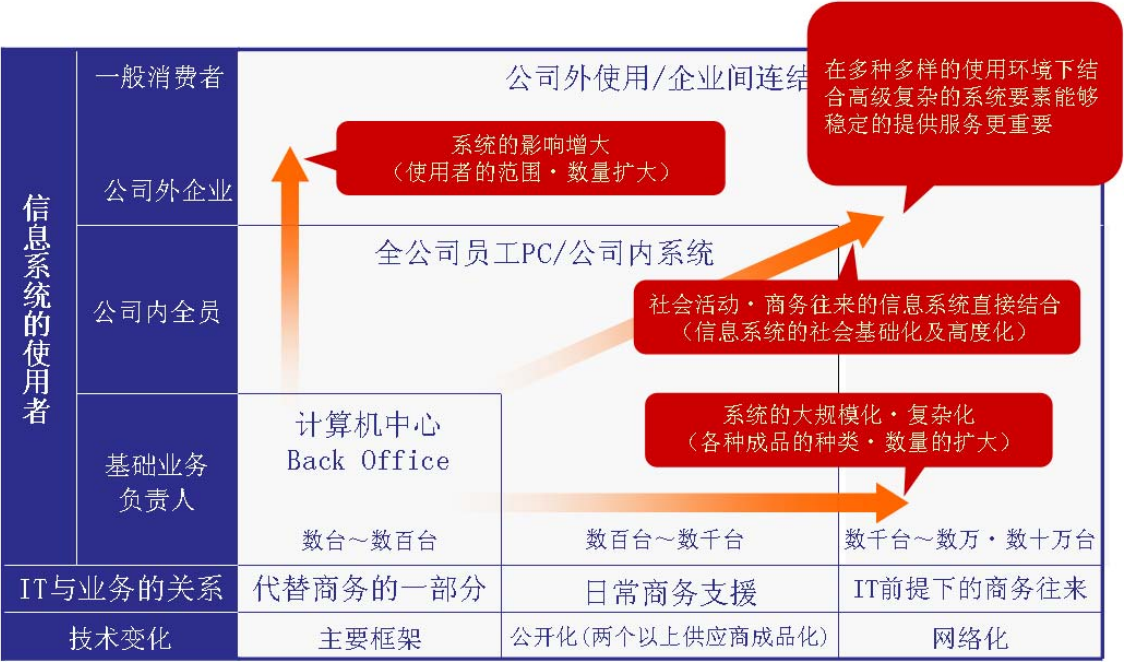


图 1.1.1 信息系统的历史性变迁

信息系统是由实现各种各样业务功能的业务应用程序与支持其应用程序的系统基础等构成的（图 1.1.2）。所谓系统基础，就是对业务应用程序提供共同的服务，硬件机器、网络机器、OS、恶意软件，通过它的控制和运营的应用程序等组合而实现的。为了能够提供稳定的服务，系统基础也是非常重要的。

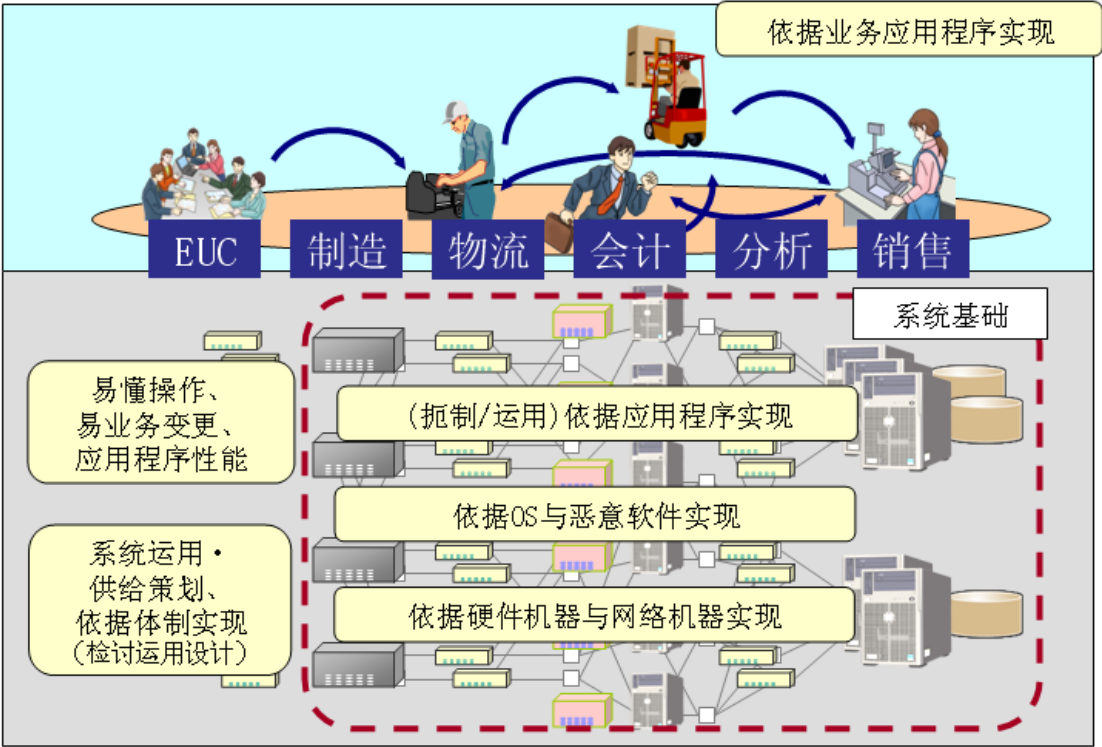


图 1.1.2 系统基础的定位

信息系统的要求大致分为两部分。（图 1.1.3）

一是，关于实现业务的要求，因现实业务功能从而被称为“功能性要求”。例如，“希望在系统上共同掌握营业信息”、“希望实行与订货、出货信息联动的库存管理”等要求。另一个是“功能要求”以外的要求被称为“非功能性要求”。例如，“系统脱机时希望能在三小时以内修复”等要求。关于系统基础的要求，主要是这个“非功能性要求”。

非功能性要求等级的目的是明确化系统基础的非功能性要求，在共有化用户/供应商之间的认知基础上，可以构建适合的信息系统、提供稳定的服务。





图 1.1.3 功能性要求、非功能性要求的效果图

### 1.2 非功能性要求的问题及非功能性要求等级的解决方法

承如上述，在开发信息系统时，用户/供应商之间持有关于非功能性要求的共同认识是非常重要的。但是，在实际信息系统开发的现场，会发生类似用户/供应商之间的必须达成共识的非功能性要求的遗漏或认识异同的差距，这种差距的发生，会阻碍信息系统的开发。

图 1.2.1 所示为上述问题。

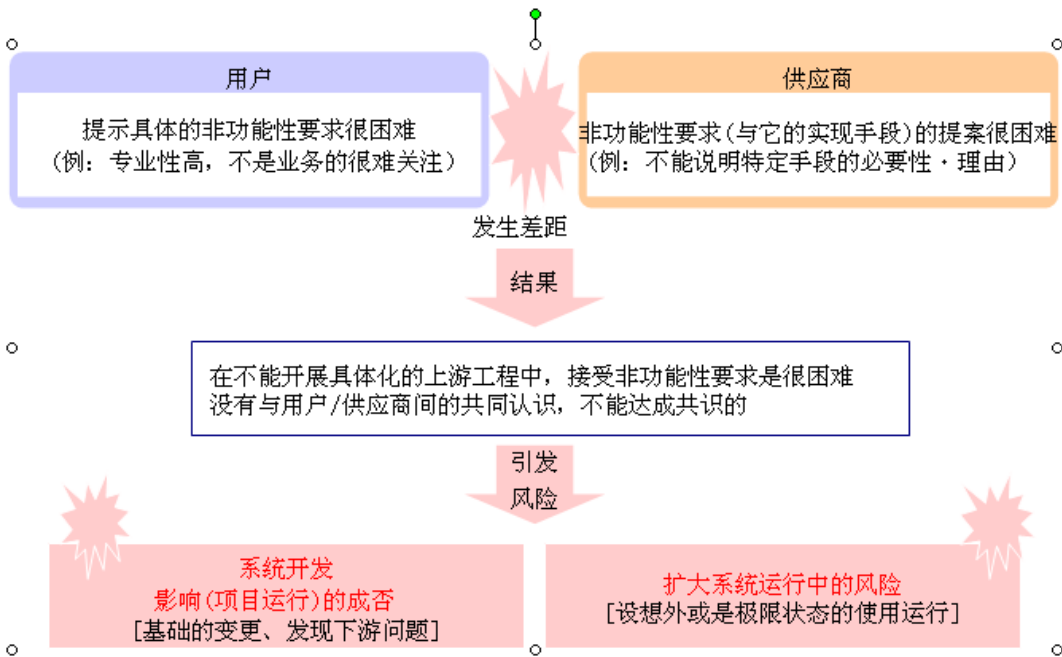


图 1.2.1 非功能性要求的问题

发生差距的理由，是因为针对非功能性要求的讨论要求具有专业性，所以对于用户来说，在开发初期，很难提出具体的非功能性要求。另外，非功能性要求是很难看清与业务有要求的要求，所以很难去关心这个要求。对一方供应商来说，就非功能性要求及其实现的手段而言，因为不能充分地说明其必然性及有效性，所以提案是很困难的。

由于发生差距，未明确非功能要求的情况下进行开发，是造成下游工程中开发及运行中故障的原因。

关于这个问题是如何通过非功能性要求等级来解决的如下所示：

- 作为用户/供应商双方可共同使用的工具、并且一般公开的资料，可以解除双方间应该达成共识的非功能性要求的遗漏及认识的不一致。
- 作为与等级详细化手順相一致的工具构成，另外包含使用方法的向导，这样用户可以快速地提出非功能性要求。
- 通过列举非功能性要求的实现等级，供应商可以具体地提示非功能性要求的实现手段。

### 1.3 非功能性要求等级的范围

#### 1.3.1 非功能性要求的定义与系统基础的关系

广义上来讲，非功能性要求是在信息系统中，想要实现功能要求以外的所有要求，也就是使用这个文字的字面意思。有关于预算等项目管理上的要求、信息系统围绕业务对象的法律・贸易规则等各种各样的定义。

非功能性要求等级是在非功能性要求中，主要根据系统基础能够实现要求的范围作为对系统基础重视的理由，在上述的要求定义中考虑在业务应用程序中对于倾向于实现要求的总是不充分的系统基础要求的确认及催促共识的必要性。

但是，非功能性要求等级中，包含对于定义系统基础要求时重要的要求项，其本身不一定必须在基础系统中实现。列举以下内容作为例子。

- 运行的要求  
运行时间等，与信息系统全部有关的，对定义功能及可用性的要求也很重要。
- 安全措施要求  
安全方针等，给其他造成影响，也有可能对系统基础中实现非功能性要求造成影响。
- 测试的要求  
是否需要测试环境，测试的范围等，有可能会对构成的系统基础的规模、体制等都造成影响。

非功能性要求等级在上游工程中，开始信息系统设计为止，作为用户/供应商之间必须对要求项的对象达成共识。

以下，在本文中没有特殊个别说明，非功能性要求用语就是本节所叙述的“关于系统基础可以实现要求”的意思。

#### 1.3.2 范围项目

非功能性要求等级是与系统基础有关的非功能性要求的范围。具体来讲，它的要求分为“可用性”、“性能・扩展性”、“运用・维护性”、“可转移性”、“安全措施”、“系统环境・低碳环保”这6个大项。<sup>1</sup>

各个大项的要求和以要求为基准的实现方法的例子在表 1.3.2.1 表示。

<sup>1</sup> 关于6个大项的整理原委，参照第3章FAQ的Q1。

表 1.3.2.1 非功能性要求等级的6大项目

非功能性要求大项	说明	要求的例子	实现方法的例子
可用性	针对系统服务可持续使用的要求	<ul style="list-style-type: none"> <li>运用计划（运作时间、停止计划等）</li> <li>故障、灾害时的操作目标</li> </ul>	<ul style="list-style-type: none"> <li>机器的双重化以及备份中心的设置</li> <li>恢复、回复方法以及体制的确立</li> </ul>
性能・扩展性	对系统性能以及将来系统扩展的要求	<ul style="list-style-type: none"> <li>对业务量及今后增加的预算估计</li> <li>系统化对象业务的处理倾向（高峰时、平时、低谷时）</li> </ul>	<ul style="list-style-type: none"> <li>性能目标值达成意识需求</li> <li>面向未来的机器、网络等的容量及配置=容量规划</li> </ul>
运用・维护性	关于系统运用和维修服务的要求	<ul style="list-style-type: none"> <li>运用过程中所需的系统运作能力</li> <li>发生问题时的对应能力</li> </ul>	<ul style="list-style-type: none"> <li>监视方法及备份方式的确立</li> <li>发生问题时的任务分配、体制、训练、手册的完备</li> </ul>
可转移性	关于对现行系统资产移动的要求	<ul style="list-style-type: none"> <li>向新系统转移期间以及转移方法</li> <li>转移对象资产的种类以及转移量</li> </ul>	<ul style="list-style-type: none"> <li>转移计划的策立、转移工具的开发</li> <li>转移体制的确立、转移演习的实施</li> </ul>
安全措施	关于确保信息系统安全性的要求	<ul style="list-style-type: none"> <li>使用限制</li> <li>防止不正当访问</li> </ul>	<ul style="list-style-type: none"> <li>访问限制、数据隐藏</li> <li>对不正当行为的追踪、监视和检测</li> <li>向实际运用者等人进行信息安全教育</li> </ul>
系统环境・低碳环保	关于系统的设置环境和低碳环保的要求	<ul style="list-style-type: none"> <li>耐震/免震、重量/空间、温度/湿度、噪音等、与系统环境有关的事项</li> <li>有关 CO<sub>2</sub> 排量以及能源消耗等与低碳环保事项</li> </ul>	<ul style="list-style-type: none"> <li>选择符合规格和电器设备相关规定的机器</li> <li>减少对环境影响的配置</li> </ul>

### 1.3.3 关于范围外的项目

非功能性要求等级中关于范围以外的项目，如表 1.3.3.1 所示。

表 1.3.3.1 范围以外的项目及其理由

No	范围外的项目	理由	例子
1	主要是选定业务应用程序的项目	与在系统中实现的非功能性要求相比，用户/供应商之间会更容易被意识到，因为配备了要求明确化的工具。	可用性、功能性、转移性
2	关于各公司个别的成品、以及解决方法的选择	个别成品与解决方法的选择是依存于信息系统的各用户，而不是由非功能性要求等级决定的。	个别具体的系统构成、构成要素、成品等

#### 1.4 非功能性要求等级的概要

本节是从非功能性要求等级的基本概念到构成非功能性要求等级的 3 个工具的使用目的及使用方法要点、工具间的关联等进行说明。

##### 1.4.1 非功能性要求等级的基本概念

###### (1) 根据级别要求项的共识

首先说明一下非功能性要求等级的基本思考方法。

非功能性要求等级是，用户/供应商双方在关于系统基础的非功能性要求上意见一致，并消除认知上的分歧为目的，

①非功能性要求的项目是用可以定量表现的指标所表示的。

②各项目是按照成本及体系结构差距设定等级。

以这样的方针为基础，整理为非功能性要求。

用户/供应商之间对非功能性要求达成共识是确定并共享上述要求项所设定等级的意思。如果要求项不是定量的而是模糊的表现定义时（例如，“满足使用者所需的性能”等）作为要求项即使相互已有认知，要求项还是会有存在异同的可能性，要求项要如何实现或者是否可以达成共识是有难度的。在设定要求项指标的同时，要事先使指标值等级化，如图 1.4.1.1 所示，在用户/供应商之间会更容易认知到实现的难易度及成本感。



图 1.4.1.1 要求项目等级化

但是等级就是共识的出发点，有一定程度的幅度，用户/供应商间有必要对于最后具体数值达成共识。

###### (2) 根据等级选定要求项

非功能性要求等级导入“等级”概念。

系统的各种各样的使用目的、规模、其系统带给社会的影响是不同的。因为这样的系统所持性质及特征的多样性，针对全部系统，是不能统一设定非功能性要求。所以作为系统的构成要素的硬件・设备、OS・中间键、运用管理的策划・体制等的配合及联合，在实现水平上

会产生差别。在开发初期这种差别是作为用户很难认知，即使供应商想要说明技术也是非常难的课题。但是在讨论系统非功能性要求时，如果可以显示具有典型模型的参考，会更容易进行非功能性要求的讨论。

因此，系统之间的差别作为等级阶段性的显示，在各个等级设定要求项的等级，早期提供用户/供应商中确认非功能性要求项的计划。

### （3）阶段的要求项详细化

非功能性要求等级是，虽然在各工具中没有限定使用用途等，但假设在用户/供应商之间、使非功能性要求阶段性、详细的达成共识各工具组成。根据各工具间的关系说明以下各工具的概要与使用目的。关于工具的详细说明请参照第2章，使用方法请参照“使用篇”。

#### 1.4.2 非功能性要求等级的构成要素・概要

构成非功能性要求等级的各工具概要及非功能性要求等级的全部构成图请阅览图1.4.2.1。

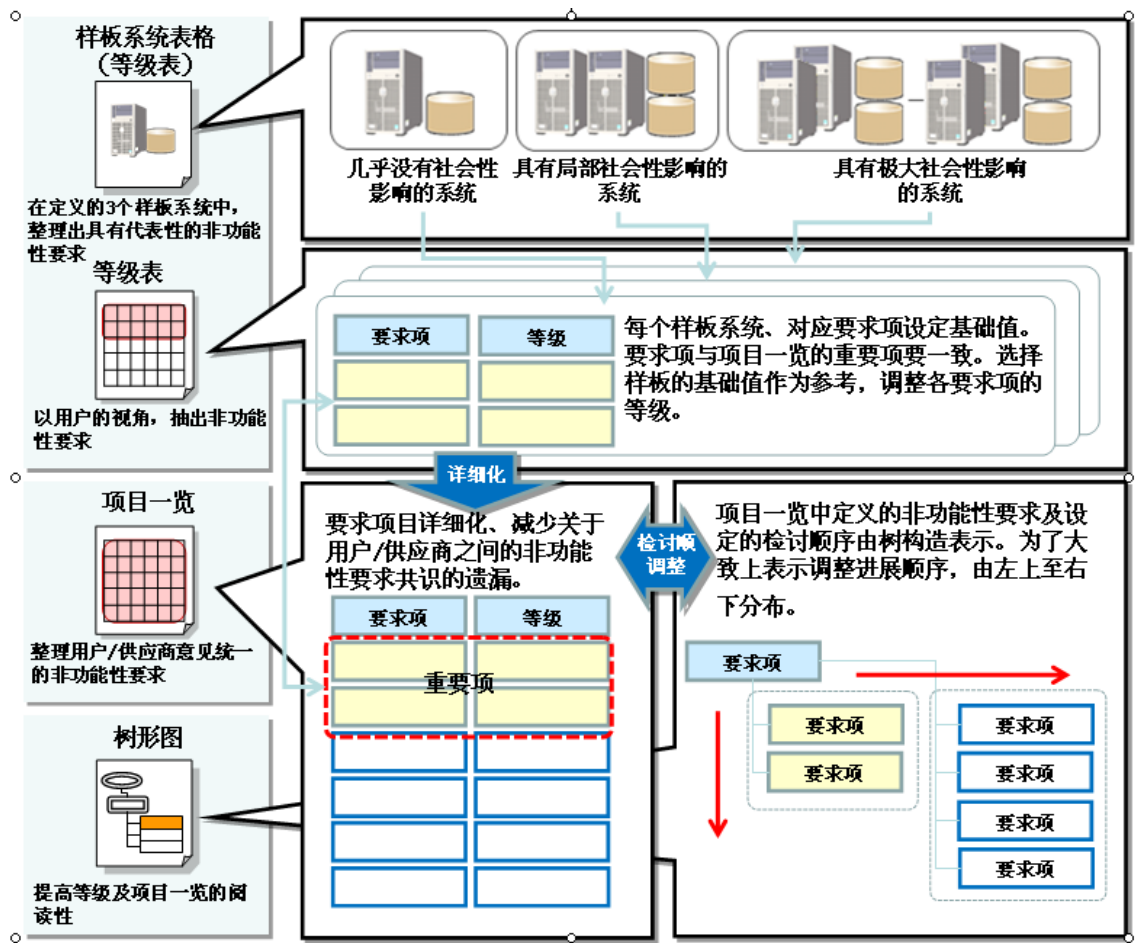


图 1.4.2.1 非功能性要求等级的概要及全部构成图

### （1）等级表

等级表是，3个“等级”其各自的非功能性要求项的等级值来定义的。在等级表中作为对象要求项是，根据用户的角度选择在品质和成本方面有很大影响而选择的项目。因此，等级表是由从项目一览中抽出的重要项的表格右侧3个“等级”所定义的等级值的组构成。

3个“等级”是，为在等级表的包含样板系统表格中，定义以下作为3个样板系统的特性。

- 几乎没有社会性影响的系统
- 具有局部社会性影响的系统
- 具有极大社会性影响的系统

在样板系统表中，以用户选定样板系统时为基准，表现出各种样板系统特征的非功能性要求为定义。关于各样板系统的具体说明及设定非功能性要求项，在第 2 章的非功能性要求等级中有详细记载。



在1个样板系统中，有选择等级和选择时的条件的记述。在选择等级中，作为基础值要设定各要求项等级的初始值。当决定非功能性要求时，结合等级表并应用，可以参考在样板系统中设定的基础值。

样板系统是非功能性要求项目的阶段性详细化在达成共识的过程中，使利用等级表的非功能性要求的选定变得容易的同时，首先，对重要的非功能性要求项目达成共识，早期控制用户/供应商之间的认识分歧为目的。

（2）项目一览

项目一览是为了可以共同认识到不要遗漏用户/供应商之间有关系统基础非功能性要求的体系化一览表。要求项如表 1.3.2.1 定义，分为6个大项。项目一览如图 1.4.2.2 所示，各大项根据要求项的单位体系的整理分类，因此提高了其网罗性。

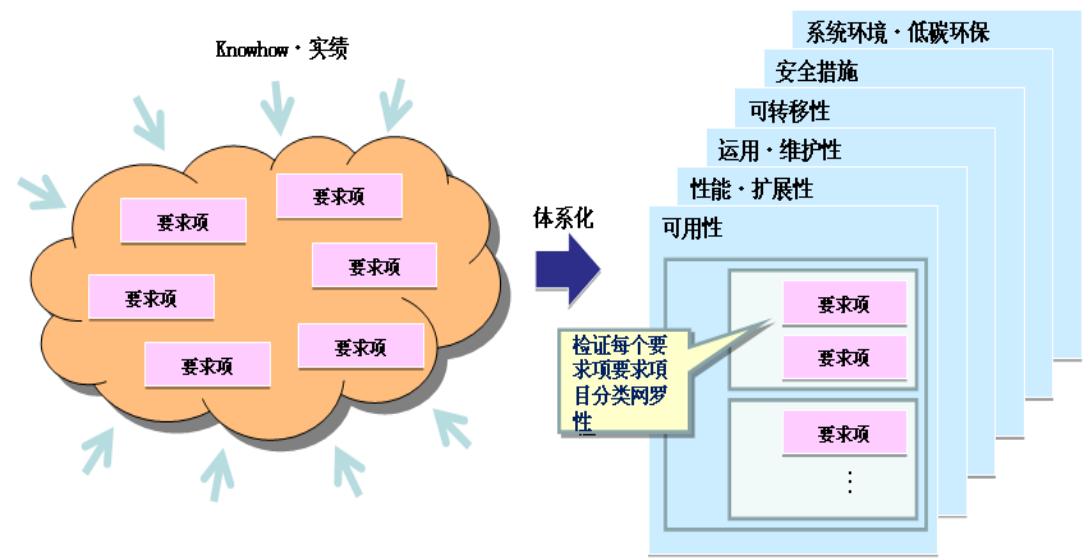


图 1.4.2.2 要求项目的体系化

在用户/供应商之间对非功能性要求达成共识的过程是多种多样的，但最终以可以确认进行共识的非功能性要求为目的。

项目一览包含以等级表定义的非功能性要求项，在阶段性详细化的过程中，假设决定等级表定的要求项以及决定详细的故障项目的使用方法。

### （3）树形图

树形图是可以提高等级表、项目一览表的阅览性、要求项的讨论顺序可视化的一个图。树形图是使用等级表及项目一览时，一并使用参照，提高非功能性要求项阶段性详细化的操作效率为目的。

例如，在使用等级表决定重要项目等级时，用户/供应商相互之间使用树形图全面查看全部非功能性要求，接着一边确定该决定哪个项目，一边可以推进操作。

## 2 非功能性要求等级的详细说明

### 2.1 非功能性要求等级的详细说明

关于非功能性要求等级的各工具，用具体的例子详细说明。

#### 2.1.1 等级表

##### (1) 样板系统的定义

非功能性要求等级，参考关于提高经济产业省的信息系统信赖性指导方针（以下简称“信赖性指导方针”）和根据参考 IPA 的重要基础信息系统信赖性研究会报告书把系统分为三个系统，<sup>2</sup>对各个系统具体定义其非功能性要求。以下，都称样板系统。样板系统的定义如图 2.1.1.1 所示。



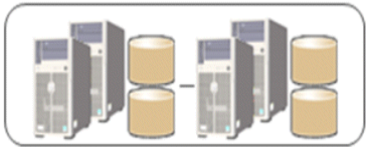
编号	样板系统名称及其图像	样板系统概要
1	几乎没有社会性影响的系统 	指的是企业的特定部门，在相对比较限制的范围内使用的系统。当其功能下降或不可使用时，对使用部门有很大影响，但除此之外是没有影响的。在此考虑的是仅限于使用小规模的网络公开系统。
2	具有局部社会性影响的系统 	指的是作为企业基干的系统，一旦其功能下降或陷入不可使用的状态，不但对该企业活动有很大的影响，连与其有合作关系的企业和客户等外部使用者也会受到影响。在此考虑的是使用限于公司内网使用的基干系统。
3	具有极大社会性影响的系统 	指的是作为国民生活与社会经济活动基础的系统，一旦其功能下降或陷入不可使用时，对于国民生活与社会经济活动将会产生极大的影响。 在此考虑的是不特定的多数人群使用的基础设施系统。

图 2.1.1.1 样板系统的定义

##### (2) 样板系统的非功能性要求项

在显示各样板系统的非功能性要求项时，因为只有名称是很难理解非功能性要求等级的，所以抽出表示样板系统特征的非功能性要求项，整理成样板系统表格。样板系统表格如图 2.1.1.2 所示。

<sup>2</sup> 在“重要基础信息系统信赖性研究会”的系统概要分析中，系统被分成 4 类，在非功能性要求等级的样板系统中，考虑到主要经济损失以及公共影响等的程度，把“人身安全影响，重大经济损失的预测系统”包含到了“具有极大社会性影响的系统”中。

	大项目	特征	无社会影响系统	限定社会影响系统	有极大社会影响系统	
样板系统概念图						
样板系统概要			企业的特定部门在比较有限的范围内使用系统。机能的下降以及造成不能使用的状态时，使用部门会有很大的影响，但不会带来其他的影响。 在这里的理想只限定为小规模的网络公开系统。	系统是作为企业活动的基本。它的机能减低以及造成无法使用的状态时，会给企业的活动带来很大的影响，同时也会给合作公司以及客户等外部使用者带来影响。	指的是作为国民生活与社会经济活动基础的系统。一旦其机能下降或输入不可利用时，对于国民经济与社会经济活动将会产生很大的影响。 在此考虑的是不特定的多数人群使用的基础设施系统。	
1	可用性	运转率	*1年中允许几天停止运转(运转率99%)。	*1年中允许几小时停止运转(运转率99.99%)。	*1年中允许几分钟停止运转(运转率99.999%)。	
2		目标恢复水准	*伴随着文件的恢复，从每周的备份文件的恢复作为目标。	*伴随着文件的恢复，恢复的目标水准是1个工作日。	*伴随着文件恢复，在几个小时内到达发生事故地点进行恢复来作为目标水准。	
3		大规模灾害	*在遇到大规模的天害时，以系统的重组作为恢复的前提。	*遇到大规模灾害时作为目标在一周以内的恢复。	*大规模灾害时(如网站要求业务的连续性) *设置备份文件中心，以应备大规模灾害。	
4		性能·扩展性	性能目标	*有粗略的性能目标，但是与其他要求相比不太重视。	*性能方面的服务等级被规定。	*性能方面的服务等级被规定。
5	扩展性		*不考虑扩展性。	*不规定系统的扩展计划。	*不规定系统的扩展计划。	
6	运用·维护性		运用时间	*仅提供业务时间内的服务。无夜间运用。	*夜间批处理完成后，确保业务开始前若干停止时间。	*以平时提供服务为前提，进行24小时365天的运用。
7			备份	*部门的管理者手动备份有必要的数据库。	*每天自动取得系统的全部备份。	*构成运用网站和同期备份网站(DR网站)。
8			运用监控	*采用硬件和软件的各种记录进行死活监控。	*对应用的各种业务功能是否正常运转进行监控。	*进行性能到资源使用状况的监控，故障的预测指出。
9			说明书	*说明书是部门的管理者独自作成。	*因为设置服务平台进行维护作业，准备运用说明书的同时也要准备维护说明书。	*定能符合本中心运用规则的运用说明书。
10			维护	*可以根据需要随时进行维护作业。	*不影响日间运用的话，可以停止系统进行维护作业。	*维护作业全部在联机状态下实施。
11	转移性	转移方式的规定	*关于转移方式的规定无特别之处(根据供应方的提案使双方意见达成一致)。	*以业务的效率化为目标，积极地进行现场化和应用的变更。	*为减少转移风险，进行阶段性转移。	
12		转移日程	*转移的日程要充分确保。	*进行转移的系统可能停止。	*转移的停止时间设置到最小限度。	
13		设备·数据	*设备和数据作为新建构筑。	*有设备或数据的变更。	*有设备或数据的转移，但是数据库构造为了保证数据的连续性和与其它系统的亲和性，不进行积极变更。	
14	安全措施		重要资产的公开范围	*持有应该实施安全对策的重要资产，但是仅和指定对方有关。(重要资产是指个人信息、敏感信息、变卖性高的信息等高安全性的信息资产)	*持有应该实施安全对策的重要资产，对不指定的多数使用者提供服务。	
15	系统环境·生态		限制	*无法律或条例等限制。	*有一些法律或条例等的限制。	*有法律或条例等的条件限制。
16			抗震	*抗震的最低级别是必要的。	*抗震的通常级别的对策是必要的。	*抗震的高等级是必要的。

图 2. 1. 1. 2 样板系统表格

表 2. 1. 1. 1 汇总每个大项的样板系统特点。

表 2. 1. 1. 1 样板系统的特点

大项	特点性非功能性要求
可用性	运作率、目标恢复水准、大规模灾害
性能·扩展性	性能目标、扩展性
运用·维护性	运用时间、备份、运用监视、指南、维护
可转移性	转移方式的规定、转移日程、设备、数据
安全措施	重要资产的公开范围
系统环境·低碳环保	限制、防震

样板系统表格是提供了图 2. 1. 1. 2 所表示的包含在等级表中的东西，阶段性详细化的活用第一阶段。关于阶段性详细化，请参照《使用篇》1. 1 节（1）。

（3）等级表的例子

等级表是从项目一览中抽出重要项目的表右侧 3 个样板系统对应定义的等级的形式。等级表的例子由图 2. 1. 1. 3 与 2. 1. 1. 4 来表示。

本项说明的是关于扩大等级定义的图 2. 1. 1. 4。

根据有关等级表的样板系统的技术，左侧列、除去重要项目列的有无，与项目一览是一样

的。关于项目一览的各项说明在 2.1.2 章节。

图 2.1.1.3 等级表的例 (全部)

图 2.1.1.4 等级表的例 (扩大等级定义)

#### （4）等级定义列的说明

各列说明如下。

##### （a）选择等级

从每个非功能性要求定义等级中，设定适当的样板系统所选择的等级。0-5 表示等级值与相对应等级的说明构成。在这里选择的等级值称为基础值。

基础值原则上是由左向右等级递增，但是也有一部分的测量标准的等级是反方向的或者变为同等级的情况。

等级为反方向的测量标准，是因为在定义每个样板系统的特征时，要结合样板系统的名字特征来定义。例如，“D.4.1.2 转移数据形式”对于有转移性的设备与数据，在具有极大社会性影响系统的情况下，定义为重视数据的持续性而不能随意变更，而在具有局部社会性影响系统中定义为有数据的变更，所以具有局部社会性影响的系统的选择等级会增高。

一方面，是因为所有同等级的测量标准作为系统基础值，不论在任何系统中都同等，但是不确定时风险极大的等级定义为测量标准。例如，“B.1.1.3 数据量”在要件定义时必须决定，所以全部等级定义为 0。

##### （b）选择时的条件

选择基础值时的条件。假设只用基础值不能适当的提示实现的系统非功能性要求时就用“－”“＋”来表示基础值变更的条件。

想要降低对象系统的非功能性要求等级，用“－”来确认条件，反之，要升高非功能性要求等级时，用“＋”来确认条件的基础上调整等级。

#### （5）重要项选择的原委

项目一览是在列表的非功能性要求项的工具中，有 236 个测量标准。这里的测量标准有的决定顺序不同，有的对于系统基础的风险度不同，所以需要进行分组。还有就是，考虑到由于项目数多所以探讨时间较长，所以选择了测量标准。这里定义为重要项。关于重要项的选择，对成本和品质影响程度大的测量标准，从用户与供应商两方面角度进行评估选择。<sup>3</sup>

#### （6）等级表的活用概念与效果

对于用户提示的要求等级，供应商的回执预算与实际预算不相吻合时，假设变更选择等级来要求再次预算的循环。这种情况下视觉上会易于确认，以超出成本为理由变更最初的非功能性要求时系统基础是如何变化的，

#### （7）等级表的编排

等级表是使用三个样板系统定义基础值，为了让用户/供应商能更好地活用等级表，也可

---

<sup>3</sup> 评估的原委参照非功能性要求等级“用户观点讨论委员会”报告书。

以把自己组织固有的样板系统追加到等级表。例如，“为××公司内部系统的样板系统”、“为学校图书馆管理系统的样板系统”等。利用实际运行的系统定义等级表，可以更精密地制定许多相似系统的非功能性要求。

2.1.2 项目一览

(1) 项目一览的例子

项目一览，是在系统的开发与运行的基础上，为了判断有关系统基础，供应商与用户确认非功能性要求项目的清单，由编号、大项、中项、小项、小项说明、重复项、重要项、测量标准（指标）、等级、对运用成本的影响、备考构成。图 2.1.2.1 表示项目一览的例子。

项番	大项目	中项目	小项目	小项目说明	重复项目	重要项目	等级等级 (指标)	等级						对运用成本的影响	备考
								0	1	2	3	4	5		
A.1.1.1	可用性	持续性	运用计划表	关于系统运用时间中止运用时的增大倍率。	○	○	运用时间(平常)	无规定	工作时间内(9点~17点)	只在夜间停止(9点~21点)	有1小时左右的停止(9点~次日0点)	有一定的停止(9点~次日0点35分)	24小时无停止		【重要项目】 C.1.1.1. 运用时的系统可用性实现水准的同时，也是关于讨论运用、保存性的开发成本和运用成本所必须的项目，也包含了可用性与运用、保存性这两点。  【测量等级】 运用时的系统性能/包括统一处理系统运转时扩展。
A.1.1.2					○	○	运用时间(特定日)	无规定	工作时间内(9点~17点)	只在夜间停止(9点~21点)	1小时左右的停止(9点~次日0点)	有一定的停止(9点~次日0点35分)	24小时无停止		【重要项目】 C.1.1.2. 运用时的系统可用性实现水准的同时，也是关于讨论运用、保存性的开发成本和运用成本所必须的项目，也包含了可用性与运用、保存性这两点。  【测量等级】 特定日系统和假日/节假日水月月初等与平常运用日程所不同的日程定义，当特定日多数存在时，每个等级值都需要调整(例：「星期一」是周五为等级2，是周六日为等级3，「平常的等级为C」，每月1号是重开日的系统，所以该天的等级为D)等。
A.1.1.3					○	○	有无计划停止	有计划停止(可变更运用日程)	有计划停止(可变更运用日程)	有计划停止(可变更运用日程)	无计划停止			○	【重要项目】 C.2.1.1. 是否将计划停止通报，运用时的系统可用性实现水准的同时，也是关于讨论运用、保存性的开发成本和运用成本所必须的项目，也包含了可用性与运用、保存性这两点。

图 2.1.2.1 项目一览的例子

(2) 项目一览构成列的说明

以下，各项目按照从左开始的顺序进行说明。

(a) 编号

表示大项、中项、小项、测量标准的连续的编号。只有大项是用英文字母(A~F)表示，中项到测量标准都是用区间区分的连续编号来表示的。

(b) 大项

体系地整理非功能性要求时的最广泛的分类。

(c) 中项

须用统一单位探讨小项目的单位汇总的分类。

(d) 小项

表示用户与供应商之间对非功能性要求项目的共识。

(e) 小项说明

小项的内容与思考方法的说明。

(f) 重复项

大项之间重复的项目。非功能性要求等级中，假设每个大项的探讨对象与探讨顺序

不同，根据各种大项的观点选择项目，所以存在重复。

归纳于某一大项以防止探讨遗漏的同时，在探讨全部汇总时，本列中可以判断是否有重复项，所以可以防止重复探讨。

(g) 重要项

在探讨非功能性要求上，对品质与成本有极大影响的项目。被选为重要项的项目是作为构成等级表项目使用的。

(h) 测量标准（指标）

为定量表现小项的指标。根据系统的构成，对于 1 个测量标准，必要对复数等级达成共识。

例如，“B.2.1.1 平时回应遵守率”不是规定系统全部的遵守率，而是多用于对应服务的重要度与使用频度，规定每个服务的遵守率。

(i) 等级

作为测量标准的评估轴，通常取值整理为等级 0 到等级 5 这 6 个阶段的项目。等级差表示体系结构中存在差距，表示为等级越大实现的难易度越高，一般的开发成本也会提高。

开发成本是从要件定义开始到系统完成的服务期间所产生的成本，包含了硬件、OS 与中间键、系统设计、导入时作业等关于系统基础的所有成本。

此外，等级值是每个测量标准独立设定的。也就是说在所有的测量标准中，即使选择同等级也没有其特别的含义。例如，等级 3 不会就成为标准系统，等级 4 不会就成为基础系统，等级 5 不会就成为高度的社会基础系统等。

等级的阶段如果不满足于这 6 个等级的情况，在图中靠左记述。

(j) 对运用成本的影响

因投入开发成本而可能降低运用成本的测量标准。

运用成本是从开始服务时，进行系统的维护与管理而产生的成本。包括运用担当者的人工费、硬件与中间键的维护费、易耗品费等。对运用成本的影响栏中画○的测量标准表现开发成本与运用成本可能有两方面权衡关系。例如，参照“C.1.2.3 备份自动化的范围”的测量标准，在对运用成本的影响栏中划有○。与等级 0 的成为“手动进行全部步骤”相比，等级 3 的“自动进行全部”中由于编入自动化功能而增大开发成本，运行时减少了人员，所以削减了运行成本。

进行等级选择时，请注意对运用成本的影响栏，在填写○的情况下，考虑对于构造后的运用成本与系统的运行周期的是必要的。

(k) 备考

每个测量标准的补充说明。记述了在项目一览中不能完全表现的部分。特别是，对于以下的内容，重点记述。

- 复数的大项目中有相同项目时的（重复项目）想法



- 对运用成本的影响的具体内容说明

另外，为清楚记载备考列的内容对应那一列，用以下的书写方法来记述。

- “测量标准”“等级”等这样的列名用“”表示。
- 特定的等级说明时，用“等级 0”来表示。

### （3）关于非功能性要求等级的等级

等级表与项目一览中所记载的等级，原则上设定为从 0 开始数值越大开发成本越高。

关于一部分的测量标准，用等级 0 和等级 1 这两个值表现的。原则上这两个值的测量标准也是等级越高，开发成本越大。但是，因为有两个值，所以还存在很难体验到成本感的测量标准。这种情况从以下 3 个观点来决定评估等级。

- ① 表现法律上的限制与对策实施的有无等情况的“单纯二值”
- ② 不能明确具体值的情况下，假设其风险的“风险顺序”
- ③ 考虑到实现难度的“难易度顺序”

综上所述，也许很难直接地表象开发成本，但如果有法律与条例、同行业界的规定等以外限制，开发成本就很容易增加，此外如果没有提出具体的要求，对于系统的风险就变大，开发成本增大的可能性也变高。可以说如果要求的复杂难易度变高，其设计的难易度也将变高，成本很容易增大。

等级是用户与供应商对于非功能性要求，按照可以正确共识的代表值所设定的，根据项目，希望的不仅是等级的选择，还有决定具体值并达成共识。例如，在“A.1.1.1 运用时间（平时）”的等级 1 中“工作时间内”的定义是根据用户与每个系统的不同，不一定与等级中的“9 点～17 点”一致。此外，“A.1.2.2 服务转换时间”的等级 1 是不满 24 小时，等级 2 是不满 2 小时，也要考虑到这之间希望设定时间的情况。

## 2.1.3 树形图

### （1）树形图的定义

树形图是，为提高等级表与项目一览的阅读性而显示的图。

树形图上的项目，大致表示用户/供应商之间调整进展顺序一样，左上至右下配置。虽然没有严密的定义，由左向右的流程大致表示中项的探讨顺序，由上至下的流程表示各小项单位的探讨顺序。

易于并用测量标准附加编号与其他工具，重要项用网状来表示测量标准以区别于其他测量标准。

图 2.1.3.1 表示树形图的例。

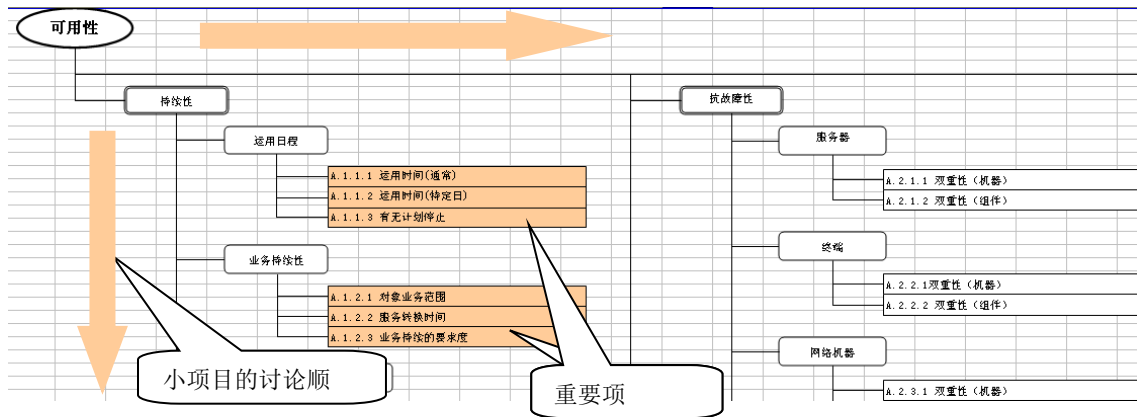


图2.1.3.1 树型图的例子

## (2) 树形图的使用方法

探讨非功能性要求时，适用于为了确认全部内容。

具体来讲，活用于各大项的测量标准的探讨顺序与重要项在一张表上就可以阅览，可以确认非功能性要求探讨时的推进方法、也可以确认探讨进展的范围等。

## 2.2 各大项的概要与注意事项

关于非功能性要求的各大项目，以下分别表示概要与注意事项。

### 2.2.1 可用性

#### (1) 概要

可用性是针对系统可持续使用的要求。也就是希望可以持续没有系统问题的服务。但是系统会发生像硬件的故障与包含 OS 的软件原因的故障、灾害等，因各种各样的原因发生不可预期的服务停止。为了如何防止服务的停止或发生服务停止时影响范围最小化而保证系统的运行品质，作为可用性来探讨。

可用性，由“连续性”、“耐故障性”、“灾害对策”、“恢复性”等 4 个中项构成。

#### (2) 注意事项

“连续性”是探讨可用性中的基本要求，由小项“运用日程”、“业务连续性”、“目标恢复水准”、“运行率”等 4 部分定义而成。在这些小项里包含的测量标准就是全部重要项。为了明确可用性要求，有必要明确在什么状态下可以运行系统的定义与故障发生时的恢复目标。前者是确认小项“运用日程”与小项“业务连续性”的测量标准“对象业务范围”等，后者是确认小项“目标恢复水准”、小项“业务连续性”的测量标准“服务转换时间”等。最终用这些定义来要求运作率。系统的运作定义不同，要求运作率也会变化，所以明确这些定义很重要。运作率实际上是从系统运作的实绩等计算而来，也成为要求可用性时的大致目标，作

为“连续性”的重要项目，定义为小项“运行率”。测量标准“运行率”，各等级值作为数值出现，置换为业务连续到什么程度的要求来进行讨论。请参考在等级表及项目一览“运行率”的备考栏中记载的大致目标。

“耐故障性”是对于故障耐性方面的要求，以系统构成要素的单位分类。“耐故障性”的各项有必要讨论用“连续性”确认的内容。不考虑“连续性”要求，只注意讨论“耐故障性”，有需要注意用户所期待系统信赖性与供应商提案对策发生的歧义。例如，在“连续性”的小项“目标恢复水准（业务停止时）的测量标准《RLO（目标恢复等级）》”中，所要求的等级只是作为特定业务来看。在这种情况下，服务器的双重化，是希望重要的业务可以运行特定的服务器双重化。但是作为小项“业务连续性”的测量标准“服务转换时间”，要求不满60秒的情况下，从“耐故障性”的观点看，要提高信赖性，选择所有的服务器双重化，成为超过“连续性”的要求的系统结构。为了不发生这种要求去对策认识上的分歧，要求确认关于各种项目的要求等级并需要双方就系统的结构达成意见统一。

此外，“耐故障性”的双重化项目分为机器等级与机器内组件等级。在可用性要求低的系统中经常忽略单一服务器结构的耐故障性要求，这种分类就是作为防止这样遗漏为目的。例如，作为没有双重化的单一服务器结构，如果发生了硬件故障等，即使恢复需要时间，还是可以继续恢复服务。因为，即使服务器停止了，也要确保不丢失数据，必须实施存取数据硬盘双重结构等最低限度对策。机器的双重化也就是统一的项目，有需要注意不要漏掉部分的对应。

“灾害对策”，在关于耐故障性要求中，特别是对于大规模灾害的要求项。这个项目是在系统构成的基础上，对服务器与存储器的构成造成影响。尽管初期不需要向远地进行备份，但是如果将来有必要进行备份的情况下，为了能够实现还是有必要从开始就选择这种装置。如果选择实现不了的装置，最坏的情况就是由于置换其装置而发生重复投资。在讨论业务的连续性基础上，是否考虑灾害对策成为在成本上占有较大比重的一个议题。

“恢复性”是故障发生时，系统恢复，能够恢复影响数据能力与关于投入其必要人力的要求项目，定义为小项“恢复作业”、“可用性确认”。由于“连续性”的讨论明确目标恢复水准。这个项目是以明确在实施恢复水准时需要的解决方法及人力为目的。

“恢复作业”是从备份开始的恢复作业到哪里为止是否自动化的项目，和在业务停止期间是否能够使用预备代替业务构成，成为不论运用、维护性与重复项。

“可用性确认”是作为可用性所要求的项目，要明确系统是否可以实现的确认范围的项目。实际进行时模拟故障的发生，确认每个的动作是否通过要求，有时也存在确认难的情况。根据系统的规模，有关确认作业的成本也会增大。为此，早期调整确认范围变得尤为重要。

## 2.2.2 性能・扩展性

### (1) 概要

性能・扩展性是有关系统性能与将来的系统扩展的要求。在提供服务时，显示是否有效的使用资源的性能。主要是表现在响应与一定时间内处理能力单位的要求。响应是接受服务一方从提出要求开始直到接受服务为止的时间，表示每单位时间内处理程序接受某种程度服务的量。要求不明确时，有时变成速度缓慢又不耐用的系统，有时被导入必要以上高功能系统，因此变得很重要。因为系统的结构各种各样，所以有必要明确制定响应与在一定时间内处理能力单位时的用语定义。

系统一旦构造，就会长期使用，因在这期间使用者数量与归纳数据量等增多导致系统的资源不足，就会使系统失去其本来的作用。作为对策，就有必要考虑扩展性。具有代表性的扩展性例子，把每个资源更换到更大的东西（提高规模）、追加服务器与机器（降低规模）。在要件定义时，因为有了预估所以易于制定机器增设的计划，视为预先准备充分的机器构成，有可能在增设时降低成本。

性能・扩展性是由作为前提条件的“业务处理量”、有关性能要求的“性能目标值”、有关扩展性要求的“资源扩展性”、辅助要求项目的“性能品质保证”等4个中项构成。

### (2) 注意事项

有关性能・扩展性非功能性要求达到共识时，一般都是最先决定“业务处理量”。业务虽然可能被认为与功能性要求一样，但在决定系统基础的非功能性要求上很重要，特别是性能与扩展性上是不能缺少的确认项目。对象系统在什么样的系统中，有必要决定在其基础上作为微略变化业务量的小项“平时的业务量”与作为在系统使用期间业务量增加程度的“业务量增大度”是必要的。即使在不明白“平时的业务量”与“业务量增大度”时，也要明确不明白理由与可能决定时期，假设具有某种程度余地的值是重要的。在这里列举了测量标准“用户数”、“同时访问数量”、“数据量”、“在线请求件数”、“统一处理件数”、“业务功能数”这6个，对应系统的特性进行的选择与追加，使得扩展性要求变得明确。

“性能目标值”考虑作为前提的业务处理量，有必要设定系统的处理形态、高峰特性与低谷时的性能目标。

依据统一处理与在线的处理形态不同，必须考虑的要点也不同。举小项“统一处理回应”为例子，在统一处理上，立足于处理时间长，作为回应目标值表示处理遵守程度，决定在规定时间内是否可以处理，是否在故障发生时再次实行的余地等。

一方面，小项“在线回应”，系统全体中并不是设定1个值，而是基于参照系与更新系的差异和系统的重要性来表示每个处理遵守率，确定符合处理的百分之几在规定时间内，从而可以规定在系统中适合的性能目标值。目标设定出现错误的话，系统的处理能力不足而无法提供足够的服务，或相反构筑出必要以上的高成本系统。

为了规定高峰时的性能目标，考虑每回处理与平时相比处理量增加到哪种程度，可否预测到达高峰的频度与时间带等。为了制定低谷时的性能目标，每回处理，确认好优先度与重要度。

“资源扩展性”规定在系统运行时有哪些资源被使用，首先决定以不同的角度考虑哪个有多少空白。表示有无空白是，根据在服务开始时的使用率与是否在客观上增设资源可能性的小项“扩展性”、“内存扩展性”、“磁盘扩展性”来确认。如果有打印机与中间键等其他资源时，推荐根据需要相应地追加。有必要配合系统完善，计划性地构造规模扩大与规模缩小的结构。

“性能质量保证”是探讨提高性能质量的解决方法。

小项“带宽保证功能的有无”是否可以保证网络的带宽，如果可以保证，希望预先确认保证在什么水平。因为画像、动画等的系统中处理的数据量增大，所以比 CPU 与内存，网络性能更会影响回应。

小项“性能测试”是规定评估“性能目标值”的实现程度的测试进行到什么程度。根据系统，有时系统构筑时的条件与运用开始的条件发生变化，所以有必要在运行后定期进行确认。

### 2.2.3 运用・维护性

#### (1) 概要

运用・维护性是有关系统运用与维护服务的要求。运用与维护的要求项目是规定系统运用方法与管理者的作业顺序的项目，对导入机器与软件的选定有很大的影响。认为与系统开发没有关系而推迟讨论，会成为引起后来“无法安排已设想的运用日程”、“无法取得必要的备份，无法恢复故障”等纠纷的原因。为了防止以上纠纷，在要件定义的阶段需要进行充分的讨论。

运用・维护性是由讨论对于平时、维护作业时、故障发生时的各种各样的运用规范的“正常运用”、“维护运用”、“故障时运用”和讨论为了实现其系统运用而制定什么样的环境与体制的“运用环境”、“支持体制”、“其他运用管理方针”等 6 个中项构成。

#### (2) 注意事项

“正常运用”在系统使用时间除了汇总有关要求项目的小项“运用时间”以外，还定义能够完成实现系统基础功能的小项“备份”、“运用监视”、“时期同步”等三个小项。小项“运用时间”有必要在运用与维护性的观点上探讨的同时也有必要在可用性观点上进行探讨，所以成为重复项。此外小项“运用时间”定义，规定正常运用日程的测量标准“运用时间（正常）”和与其不同的规定运用日程的测量标准“运用时间（特定日）”这两种。平日业务运用以外的像星期六的备份运用和星期日的计划停止似的，在正常的运用日程以外的特定日复数存在的情况下，有必要预先确认关于各个不同的特定日。

“维护运用”定义为维护小项“计划停止”、“统一处理适用方针”、“活性维护”等的系统品质而实施的维护作业方针与内容的项目。这些是左右维护作业的方法与日程的项目，对于导入机器的选定也有较大影响，所以事先决定是非常重要的。

“故障时运用”定义为决定所谓的小项“恢复作业”、“系统异常检测时的对应”、“交换用部品的确保”在决定对应系统发生故障时的项目。与“正常运用”的小项“运用时间”一样，这里小项“恢复作业”在运用与维护性和可用性中也成为重复项。导入机器与要员、部品材料的确保等及对成本有影响的项目很多，所以就可用性与运用、维护性这两方面观点有必要进行充分的讨论。

“运用环境”定义小项“开发用环境的设置”、“试验用环境的设置”、“手册标准等级”与“远程操作”等有关系统运行环境的项目。这些项目都对系统的运用方法有很大影响，在实际运用开始，可以看到遗漏的情况，所以要注意。

“支持体制”定义小项“维护契约（硬件）”和“维护契约（软件）”等与维护契约相关的项目、或者，“维护作业任务分担”、“一次对应任务分担”等与系统运用及用户/供应商之间任务分担有关的项目，还有，如“操作训练”和“定期报告会”对应用户系统运用的供应商的支持体制的项目。这些虽然总是被认为与系统开发和构筑没有直接关系而推迟讨论，但是为了确保系统的品质，必须在事前进行讨论。

“其他运用管理方针”定义小项“内部统制对应”与“服务助理”、“突发事件管理”等与ITIL 有关的项目。这里的项目是确认是否进行管理的项目，实际实施管理上，用户与供应商达成统一意见时，必须确认具体的实现方法。因为是对系统的设计与开发作业都有影响的项目，所以必须事前确认包括具体实现方法在内的事项。

## 2.2.4 可转移性

### （1）概要

可转移性是关于现运行系统资产转移的要求。面向新系统的运作，除完全按照新规的开发情况之外，必须要把现行系统的资产转移到新系统中。因为资产不能转移的话，即使系统开发完了也无法作为系统全体来利用。因此，抽出对于系统的转移有必要的要求项目并策定转移计划，准确地实施计划是非常重要的。

可转移性是，有关转移日程的“转移时间”，有关向新系统的转换方式的“转换方式”、掌握转移资产对象的“转移对象（机器）”、“转移对象（数据）”以及为了转移进行演练等的“转移计划”等5个中项所构成的。

## （2）注意事项

作为“转移时间”，从转移计划开始到系统转换为止有多长时间，在此期间进行转移作业时，是否有系统停止的可能，是否有并行运作的必要，从这些观点进行讨论。如有并行运作的必要，对并行运作的期间达成一致是非常重要的。

作为“转移方式”，存在系统有复数的地方所设置的小项“据点展开步骤数”与系统以复数业务构成时的小项“业务展开步骤数”。不论哪个情况，转移与展开越多阶段，新旧两个系统的部分性共同运行时间越长。为新旧系统的共同存在而连续运行全部系统时，考虑新旧两个系统的并行运行时，一起展开比更多阶段性展开难度要高。但是，在对象系统中根据展开时的风险，有时一起展开的难度也会很高。因此，关于转移与展开的阶段数，有必要事前考虑到关于每个对象系统据点，每个业务展开时的风险。

确认作为转移对象的“转移对象（机器）”与“转移对象（数据）”。

“转移对象（机器）”，作为小项“转移设备”在旧系统中使用过的设备与机器只对作为新系统的硬件更换而继续使用，或作为全新系统更换等，确认更换的范围尤为重要。在设备与机器进行部分更换时，对继续使用的硬件和软件，要考虑到维护支持是否可用，或者与更换的设备与机器的互换性。

“转移对象（数据）”中有测量标准“转移数据量”、“转移数据形式”、“转移媒体种类数”与“转移工具的复杂度（变换规则数）”等。特别是转移数据，数据形式与转移方不同时，形式变换用的设备与转移工具是必要的。转移工具是作为工具的复杂度以变换规则数表示，对变换时的规则增加与工具开发量和变换作业时间等都有影响起重要作用。在转移时必须使用转移媒体的每个种类，如何向转移设备里安装，有必要讨论它的方法及装置。

“转移计划”，确认小项“转移作业分担”、“试运行”、“应对故障”。

关于转移作业的用户与供应商的分担，特别是关于转移对象数据的旧系统转移对象数据的调查、转移数据的抽出与变换、向正式运行系统中的导入与确认等，规定其作业分担很重要。有关最终转移结果，用户必须进行确认。

外部联合试运行，与正常试运行一样明确对象外部系统，有必要对试运行的范围、环境与次数进行规定。并且在外部系统与其连接方法发生变更时，在新系统中新旧两个方法的支持。在这时，为了减少系统转移风险，有必要确认两种连接方法并计划外部联合试运行。

小项“故障应对”是预先制定在转移实施场所驻在人员与恢复断点的对应计划等的项目。万一发生故障时，以能够顺利进行为目的，确认其内容是很重要的。

## 2.2.5 安全措施

### （1）概要

安全措施就是有关确保构筑信息系统安全性的要求。如果没有采取适当的安全措施对策，就会出现威胁，会对使用信息系统业务的完成产生障碍，其结果恐怕会直接的、间接的带来较大的社会与经济上的损失。为了避免这种情况的发生，要明确对应构筑的信息系统必须讨论的关于安全措施的非功能性要求，为了不发生遗漏有讨论的必要性。

此外，关于安全措施的非功能性要求很多是影响信息系统的性能的要求。例如，像密码处理，就有许多在原有的信息处理上增加负荷这样的要求。讨论关于安全措施的非功能性要求时，重要的是要同时讨论性能与扩展性的非功能性要求。

安全措施，有关对象系统的安全措施的前提条件与制约条件“前提条件・制约条件”、有关开发时与运用时的安全管理项目“安全措施风险分析”、“安全措施诊断”、“安全措施风险管理”、实现安全措施对策的功能“访问・使用限制”、“数据的隐藏”、“非法跟踪・监视”、根据功能组合安全对策的主要模板“网络对策”、“恶意软件对策”、“Web 对策”等中项所构成。

## （2）注意事项

“前提条件・制约条件”是指，对信息系统实施安全对策时，有关确认主要在法律与同行业界中有关信息安全的基准、<sup>4</sup> 指导方针、在企业中称为信息安全措施方针的组织规定的项目。确认作为“前提条件・制约条件”规定、法律、指导方针等，遵从这些条件，有必要决定有关安全措施非功能性要求项目的等级。例如，根据遵循的规定，规定与小项“认证功能”、“数据密码化”等相符合明确的安全措施的情况。此时，有必要根据其规定所表示的安全措施必要条件与选择等级之间不产生矛盾而规定非功能性要求。在样板系统中，表示不受有关安全措施的业界基准与企业方针等的影响这样广泛通用的例子，也表示了全部没有规定的例子。因此，等级表的“E. 1. 1. 1 必须遵守社内规定，规则、法律、指导方针的有无”的基础值，在全部系统中作为等级 0（没有）存在。对应业界的基准与企业的方针，确认是否必须遵守规程、法律、指导方针等，如果有的话，有必要决定为了满足其要求规定的等级。

“安全措施风险分析”是在开发信息系统时，筛选出潜在的威胁，为了明确安全措施的实施范围进行风险分析的项目。讨论“安全措施风险分析”时，在信息系统中筛选出使用资产（硬件・软件资产以及信息资产），确认什么资产是保护对象。在对安全措施有关的非功能性要求达成共识时，不仅是对在项目一览所表示的安全措施对策实施的有无，也要对有关不实施安全措施对策的项目（由于不实施安全措施对策残存的安全措施风险）进行共识。

“安全措施诊断”是，对于开发信息系统实施安全措施特化试验的项目达成共识。在讨论“安全诊断”时，不仅对使用工具与评论方法等，更要对具体的诊断方法与诊断范围进行讨论。

---

<sup>4</sup> 有《政府机关信息安全对策统一基准》、《金融机关等计算机安全对策基准》、《Payment Card Industry Data Security Standard (PCI DSS)》。参照 5.2.6 项~5.2.8 项。



“安全措施风险管理”是，对系统运用后所发现的威胁与脆弱性的对应方针的项目达成共识。“安全措施风险管理”因含安全措施统一处理的适用范围与时机项目，所以有必要探讨有关运用与维护性统一处理全部的适用范围与时机。

“访问・使用限制”在开发信息系统中，对于处理资产的访问与使用限制的项目达成共识。讨论“访问・使用限制”时，要对每个实施场所（服务器、存储器等）的对策进行讨论。

“数据的隐藏”在开发系统实施流通与积累信息隐藏的项目中达成共识。讨论“数据的秘匿”时，成为秘匿对象的信息资产以及实施场所一并讨论。为了秘匿而进行密码处理时，要考虑对性能的影响。

“非法追踪・监视”，对有关系统运行后发生的非法行为追踪及监视的项目达成共识。在讨论“非法追踪・监视”时，要考虑到为了检查非法行为而获取安全措施日志等对性能造成的影响。

“网络对策”是，定义网络的安全措施对策的项目。“网络对策”是，导入为了拦截非法通信的制约与系统内非法行为及检查通信的方法，由于介入网络的攻击，讨论网络拥挤的对策。作为网络拥挤对策，用服务器处理能力增强应对时，在性能与扩展性中，与决定服务器的处理能力资源扩展性等的项目一同讨论。

“恶意软件对策”是，定义有关电脑病毒、蠕虫等恶意软件的安全对策的项目。讨论“恶意软件对策”时，考虑到同时检查恶意软件对性能造成的影响。

“Web 对策”是，定义针对 Web 应用程序脆弱性的安全对策的项目。讨论“Web 对策”时、要考虑到用 WAF（Web Application Firewall）同时进行监视对性能的影响。

## 2.2.6 系统环境・低碳环保

### （1）概要

系统环境・低碳环保是指对于系统设置环境和低碳环保的要求。前者的系统环境部分是由设置系统时所约定的“系统制约/前提条件”或者围绕系统的使用者和地域性扩张等的“系统特征”，“适合规格”，“机械材料设置环境条件”所构成。这些项目因事后即使知道有规定也很难变更，因此定义中有遗漏的话，则容易发生因需求定义的变更而导致很大分歧的重要项目。

另外，后者低碳环保部分是由“环境管理”所构成。主要是指物量的废弃或减少 CO<sub>2</sub> 排出量、提高能量消费效率等。近年来，全球出现了提出 CO<sub>2</sub> 消减业务化或规定方针政策的国家或地区，使此项目尤为重要。

## （2）注意事项

“系统制约/前提条件”中定义“构造时的制约条件”，“运用时的制约条件”两个小项。如果存在可以成为构造时及运用时制约条件的组织内的规定或法令・条例等，就需要依照规定探讨。如果不注意这些规则而构造系统的话，要么重新变更为依照规定的构造，要么据需要满足条件进行再设计。例如，有关进出管理规定，并根据此规定设定在数据中心的系统中，不管运用中需不需要遥控操作，如果在要件定义阶段遗漏这各个条件就吻合上述的案例。

“系统特性”定义为“用户数”、“客户数”、“据点数”、“地域性扩张”、“特定制品指定”、“系统利用范围”、“复数语言对应”等小项。用户/供应商之间早期就达成共识在构造系统中是非常重要的。因为，这些项目会成为决定系统规模和特性的要件。例如，如果没有正确定义用户数或客户数，或者，遗漏系统运转周期中未来增加部分，可能会引起资源问题。这些项目因早期进行共识，来支持系统特性。

“适合规格”定义为“制品安全规格”、“环境保护”、“电磁干扰”等 3 个小项。根据系统的用途和设置环境・运用环境的不同，要求产品满足一定的基准。产品的安全性和对机器发出电磁波的限制，还有特定有害物质的使用限制规定等会包含在其要求中，因此要确认对所构成机器的要求。

“机械材料设置环境条件”定义为“耐震/免震”、“空间”、“重量”、“电器设备适用性”、“温度（区域）”、“湿度（区域）”、“空调性能”等 7 个小项。这些项目是在需求定义阶段在定义中容易被遗漏的项目。比如，从需求定义阶段到设置环境不进行充分探讨的话，一旦想要设置的时候，会出现无法满足地面负荷条件，或因空间关系无法设置等情况。

“环境管理”定义为“控制环境负荷的技巧”、“能量消费效率”、“CO<sub>2</sub> 排出量”、“低噪音”等 4 个关于低碳环保的小项。关于低碳环保，最近官公厅领头实施绿色筹措的企业越来越多。还有，今后可能会出现因对应碳素税等法律性而突出的现象。并且，低碳环保具有体现企业的社会性责任（CSR）或公正透明健全的贸易方式的观点，因此可以想到今后企业在取得社会信赖中变得越来越重要。

## 3 FAQ

### 【非功能性要求等级的范围】

**Q1：非功能性要求等级为什么要选择这 6 个项目呢？**

A1：在定义系统基础的时候，我们根据各种标准类别和实例，想要确认用户的要求，以由下至上进行了集中整理，把他们分为 6 个大项。分类时也参照了 ISO/IEC9126 等标准类别，非功能性要求等级主要是为了实现系统基础，集中于非功能性要求上，他们的

标准分类并没有网罗所有的分类项目。

**Q2: 非功能性要求等级的范围包括应用程序的要求吗？**

A2: 功能性要求主要由业务与应用程序来实现，非功能性要求主要依赖于被称为系统基础的领域来实现。所谓系统基础，是指由服务器、存储器、网络等的硬件设施与 OS、中间键和它所控制的运行管理软件所组成的。在“非功能性要求等级”中这个系统基础以实现非功能性要求为对象，有关实现业务和应用程序功能要求是排除在范围之外的。但是，在实际的系统案件中对要求讨论时，系统基础与应用程序的界限如果不清晰的话，我们也要把这些结合起来进行讨论的案件也是存在的。为此，考虑把业务与应用程序包含在内的项目，我们应该把与系统基础的讨论有关的项目包含进范围里。（例：业务处理量、运用时间等）。

**Q3: 为什么使用“等级”这个词汇？**

A3: 等级是既表现系统的实现阶段的差距，又同时满足成为系统规格的一套要求项目的定义用语。特别是不仅仅意图表示优劣的用语，是与汽车的豪华型、经济型、运动型相近的思维方法来表现出特定要求的特定用语。

相对于信息系统而言，虽然在硬件设备、OS 中间键、运行管理的组合体制等构成要素的组合与协作的实现水准会有差距，但在开发初期，这个差距很难被使用者所认识即使作为供应商对此技术进行说明也有一定的困难。在这种情况下，作为系统间的差距用“等级”来表示阶段，在早期，用户同供应商双方以确定要求事项的讨论为目的，制作“非功能性要求等级”。

**Q4: 以非功能性要求等级作为对象的用户是指？**

A4: 非功能性要求等级，在信息系统开发程序的需求定义时，以与非功能性要求的提示、提案、决定有关的发包方、承包方双方的担当者作为对象。另外在文中，把发包方称为用户，把承包方称为供应商。具体内容参照“经营者参与企划确保要求品质第 2 版（SEC BOOKS）”，在发包方企业中把信息系统部门，假想为用户。但是，此向导，是为了方便将使用方法客观的进行说明而设定的，对谁、怎么使用非功能性要求是没有制约的。

**Q5: 非功能性要求等级是在系统运作周期的哪个时点进行使用的？**

A5: 非功能性要求等级是假设活用于在“标准框架 2007”的企划程序、需求定义程序、开发程序中的非功能性要求的处理程序与活动性。另外，在“经营者参与企划确保要求品质第 2 版（SEC BOOKS）”中，相当于被称为上游工程的“系统化的方向性”、“系统化计划”、“需求定义”。非功能性要求等级是假设用户与供应商之间与有关非功能性要求进行共识的一个工具，其内容记载在 RFP、需求定义书与预算提案这样的文书中，

作为系统设计契约也包含在共识事项中。此外，虽然主要假设在上游工程的使用，但是因为由“非功能性要求等级”整理而成的内容，考虑到在系统设计和试验中也有可能使用，所以请根据需要使用。

### 【等级表、项目一览与树形图】

#### Q6：项目一览的等级是根据什么顺序来排列的？

A6：测量标准通常把取得的值整理为从等级 0 到等级 5 这 6 个阶段。等级越大难度越高，一般来讲也表示开发成本会变高。互相比邻的等级值之间，基础设施的差距是存在的。这样来被设定的，一旦等级值上升或是下降，要考虑到在设计与实际安装满足其结果需求的系统时，能够显示出有多少构造的变化。但是，对于一部分测量标准，也存在以等级 0 或者等级 1 这两个值来表示的情况。这些是针对表现有无法律限制的单纯二值，表示假设没有定义具体的数值的风险顺序。这些在等级值之间的构架差距不明确就会很难实际感觉到对开发成本的影响，但存在限制、高风险的一方，实现的难度也会变高，其结果就是会产生高成本的可能性，按可能性的高低来决定等级顺序。

#### Q7：大项之间存在着相同的测量标准，我们应该怎样考虑这些标准呢？

A7：非功能性要求等级，假想每个大项的讨论对象与讨论顺序都会不同，为了防止讨论有所遗漏，几个项目会存在重复的情况。那些不会分别设定数值，要把它们设定为同样的值。多数的担当者对每一个大项的探讨结果进行总结时，时间上间隔的时间点中讨论各大项目时，对于在重复项列前有标志○的项目，请选取大项之间的整合推进讨论。

#### Q8：“对运行成本的影响”表示什么？

A8：项目一览或等级表的等级表示了开发成本的高低，系统开发要不仅要对包括开发成本也要对包括运用成本的总成本来评估。开发成本是指，从需求定义后到系统开发完成开始服务的期间内所花费的费用，运行成本是指系统进入服务后为了系统的维护与管理所发生的费用。在项目一览中，被定义的要求项中，像处理自动化等这样需要开发成本但会降低运用成本的项目。对于这样开发成本与运用成本有成为协调关系的可能性的项目，要在“对运行成本的影响”栏中标记为○。因此，尽管指定开发成本高的等级也会有控制总成本的情况。

#### Q9：等级表的对象项目的重要项的选择依据是什么？

A9：在非功能性要求等级的项目一览中存在着 236 个测量标准。这些测量标准中，有的决定顺序不同，有的对系统基础的成本的影响程度不同等项目，这需要进行一定的分类。另一方面，简单地说要考虑到项目数过多而需要讨论时间也会增多的问题，来选定重要项。在选定重要项时系统的开发成本与影响品质的程度是一个大项目，需要从用户与供应商两方的视点来加以考虑。

**Q10: 树形图表示的是什么?**

A10: 树形图是为了提高等级表与项目一览的阅读性而制作的。树形图上的项目, 如大致表示用户与供应商间调整的进行顺序一样, 从左上到右下进行配置。虽然没有进行严格的定义, 但一般情况下是以从左到右的流程大致表示中项的流程、从上到下的是表各个小项的讨论顺序。像这样, 用“中项”、“小项”、“测量标准”的系统图来表示探讨顺序, 一般来说, 不使用“树形图”的文字使用的是“树系图”的标明。

**【非功能性要求等级的使用方法】**

**Q11: 在项目数很多的情况下, 一次讨论不完的应该怎样做?**

A11: 选定项目一览中重要度较高的测量标准, 从它们当中定义可以开始进行讨论的等级表。等级表不仅仅集中于重要度高的测量标准, 还假想成为样板的系统并显示出等级值选择例(基础值)。作为讨论顺序, 选定等级表中的一个样板系统来调整各个测量标准的选择等级, 从而逐渐接近目标系统的要求。

**Q12: 如果存在与自我讨论系统无关的项目, 应该如何进行处理?**

A12: 等级表与项目一览是抽出系统开发时的必要项目。记载于需求定义工程中 RFP 与预算提案, 也包含在与那一时段的共识事项。预测根据成为用户的环境与对象的系统的不同, 会产生不需要讨论的事项。在这种情况下, 不进行讨论的理由需要在用户与供应商之间达成共识。

**Q13: 在契约时点存在不能决定的项目时, 应如何解决?**

A13: 在非功能性要求等级中, 希望需求定义工程能够使项目一览中的全体的项目都达成共识。可是, 如果不是详细的设计就决定不了等诸如此类的理由, 不一定要在上游工程中就决定出所有的要求项目。关于不能决定的项目应事先进行明确决定日期与决定方法等。像这种情况需要考虑契约变更与多阶段契约。

**Q14: 开发程序过程中, 发生需求的变更应如何处理?**

A14: 非功能性要求等级假设使用于需求定义程序中, 要考虑到可以使用检测被决定的内容是否清晰的反应在了系统设计同构架内容中的用途。这样在开发程序的过程中发生需求变更的情况, 也应被充分的考虑进去。非功能性要求等级也可以作为确认和用户与供应商之间达成共识对此时需求变更内容与其影响程度的工具被使用。

**Q15: 工具的使用有什么条件?**

A15: “使用篇”与“解说篇”两篇的使用向导,“等级表”、“项目一览”、“树形图”的 3 个工具的著作权归独立行政法人 信息处理推进机构(以下简称 IPA)所有。IPA 希望此工具被广泛的使用,因此著作权设定了最低限制的使用条件,并为了可以进行自由的使用而进行了公开。另外,还提供把项目一览与等级表编辑成一个可以编辑的空白表格形式的“活用表”。

详细的使用条件请参照各个向导与工具的记载。

## 4 用语集

用语	说明
转移设备	构成基础系统的设备中，被新设备所替换的设备。
转移数据形式	依赖于应用程序的格式，表格形式或文字代码等，为转移到新系统而必须考虑的数据形式。
转移媒体种类数	现有系统的数据转移到新系统时，必须使用的媒体种类数。比如，磁带，光盘，票据等。还有，根据网络连接的数据传送也作为媒体种类包含于其中。
一次对应	信息系统或者构成信息系统的各机器和软件等的故障咨询窗口的初期调查。主要担当信息收集和问题点的区分。
事件	关于信息系统，支援担当者必须对应的故障或问题点的单位。
运用网站	设置运转系统的场所。
能量消费效率	定义为在“关于能量使用合理化的法律”（略称：省能量法）中，根据该法中的测定方法所测定的消费电力除去符合伦理性能的部分。（因此，所得值越小效率越高）。获得同等能量所需的能量越少，能量效率越高。
错误监视	检测构成系统的服务器或其他机器，或者在此运作的中间软件或应用程序等所规定的运行记录文件的信息输出发生错误的监视方式。
错误检测	保证数据完全性功能之一，检测数据错误的功能。  （关联用语） → 数据安全性
错误订正	保证数据完全性功能之一，对检测出的数据错误进行订正的功能。  （关联用语） → 数据安全性
操作	对信息系统一系列的操作。
操作训练	关于信息系统操作的训练。
线路	构成网络的传送路。
恢复性	发生故障时，把系统恢复到要求水平的能力。
外部系统	存在于开发对象系统范围外的系统（开发对象系统和相连的原有系统等）。
外部数据	外部系统所拥有的数据。有时为开发对象系统所拥有的原有统计数据，有时也是复制数据。
锁管理	用于暗号，数码签名等锁的管理。
火灾对策	为防止因火灾引起的系统故障的对策。包括检测对策，消防对策等。
活性维护	系统在运转状态下所实施的构成信息系统的机器的追加，消除及部品交换等工作。
运转时间	系统在一天中所提供服务的时间。运用时间。
运转率	系统预定提供服务的时间与实际提供服务时间的比例。运转时间率。相反，无法提供服务的时间表示为平均下降时间。还有一般运转率表示为以下形式。 运转率=MTBF/(MTBF+MTTR)  （关联用语） → MTBF(平均故障间隔) → MTTR(平均恢复时间)
雷对策	因雷产生的过电流中，保护系统的对策。
可用性	(1) 系统明示的利用条件下，显示在所规定的时点里所要求的业务实施到什么程度的能力。用于大项名的可用性定义在信赖性的意义之上。  (2) 因许可的对象（用户及程序）而被要求时，可以访问和使用的特征。
伽 (Gal)	表示加速度的CGS单位(1Gal=1cm/(sec <sup>2</sup> ))。名字来自于发现落体定律的伽里略。例如，地表的重力加速度约为980Gal。另外，与地震震度的关系是震度4(25~80Gal)，震度5(80~250Gal)，震度6(250~400Gal)，震度7(400Gal以上)。

用语	说明
监视	<p>确认信息系统本身及构成信息系统的机器，程序等对象物是否处于所期待的状态，并根据所确认的内容告知指定通知方，或其结构。</p> <p>（关联用语）  →当机监视  →错误监视  →资源监视</p>
机械材料设置环境条件	设置机械材料的建屋方所能提供的环境。具体的可容纳机械材料的重量及空间，电器设备吻合性，温度，湿度，耐震/免震对策等。
机密性	对于不允许访问某种信息的对象（用户及程序），把此信息作为利用不可或者非明示的特性。
威胁	具有引起安全措施风险可能性的，系统攻击，契机，操作・设定错误等。
业务	利用系统原有的功能，处理给与的要求。不仅包括系统原有的功能还包括因系统使用和人的活动。
业务功能数	筛选构成对象业务功能的数（依据功能构成图或功能信息关联图等）。可代用子系统数或画面数等。
业务继续性	即使没有预期灾害和故障而发生事故时，也可以通过运转可能的资源的活用或瞬时恢复等继续业务的能力。BCP（Business Continuity Plan）。
继续业务的要求度	表示对于所发生的故障，可以继续业务的程度。
业务展开步骤数	系统由复数业务所构成的场合，把业务阶段性地转移或展开到新系统时的展开阶段数。假如存在3个业务子系统，把基于业务按A业务，B业务，C业务顺序实施转移的话，业务展开步骤数为3阶段。
共用中心	大规模灾害中，不可能恢复本系统时可利用的共用的数据中心，服务器群。
据点数	为提供服务而展开的场所的数量。一般指分社，分店，店铺，工厂等设置机械材料的据点数量。
据点展开步骤数	系统被设置在复数场所时，把系统基础和数据阶段性地转移或展开到新系统时的展开阶段数。比如，把本社和分社使用的基础业务系统按本社，分社A，分社B的顺序转移的话，据点展开步骤数为3阶段。
客户数	提出服务要求的终端数。
群	提高系统的信赖性或者处理性能为目的，把复数的电脑综合为一个的结构。冷备件和热备件等方式。
绿色购入法	“不同国家关于推进环境物品等调查的法律”的略称。购买制品和服务时，认真考虑环境及购买必要性，选择尽量减少对环境有负荷作用的购买，称为绿色购入法。强制要求不同国家机关实行绿色购入的同时，也希望地方公共团体和事业者・国民努力去实行绿色购入。绿色购入不仅使消费生活等购买者自身活动变为保护环境的活动，还促进供给方企业开发环境负荷极少的制品，改变经济活动的全体。
等级	对于1个样板系统的非功能性要求的选择等级和选择时的条件组合。
等级表	关于系统基础的非功能性要求的等级表。非功能性要求等级提供3个样板系统的等级表。
计划停止	维护和检测等为目的预先预定的信息系统的停止。相反，没有预测故障而发生的信息系统停止称为计划外停止。
途径	在网络内数据流动时的正常路线。
组件	构成装置的部品。例如，服务器的话，CPU或磁盘，网络卡等。
服务器监视	对构成信息系统的服务器或者提供服务其功能的软件的监视。节点监视。
服务	给系统提供便利。系统指的是IT系统。
服务替换时间	<p>系统根据群等双重化时，从一方替换到另一方的时间。 与下降时间同等。</p> <p>（关联用语）  →运转率  →MTTR</p>
服务停止攻击	对于服务器传送大量的数据包和数据，来消耗线路容量和内存容量等，或者使CPU处于超负荷状态来降低或废止服务和系统的处理能力。
服务桌面	实施信息系统的维护，给使用者提供日常运用的服务支援的组织功能。



用语	说明
再试行	作为保证数据完整性的功能之一，当检测出错误的数据时，可以再实施处理功能的行为。比如，演算器或寄存器等的硬件命令的再试行等。  (关联用语) → 数据安全性
死活机监视	确认监视对象是否起动的监视方式。
时间指定恢复	使用备份的恢复数据作业中，在特定时期内的任意时刻恢复数据内容的功能。Point in Time Recovery (PITR)。
资产	与系统有关的硬件，软件资产，信息资产及业务。
地震对策	防止因地震引起的灾害的对策。包括耐震，免震，制震等对策。  (关联用语) → 耐震 → 免震
系统	主要是指硬件，软件，其他设备的总称。与IT系统同义。广义的系统包括人的因素，而在非功能性要求等级中使用的是不包含人因素的狭义的系统。
系统转移期间	从实现原有系统到新系统的转移作业计划到新系统实际运作为止的时间。
定期日志	在发生系统故障或处理异常时，以查明原因和恢复为目的所保存的处理履历和记录。
切断对策	关于漏电对策，防止检测出的泄漏电流流入到系统的对策。
重复项	大项中重复的项目。等级表和项目一览中重复项划为○。
重要项	探讨系统基础的非功能性要求之上，对品质和成本具有极大影响的项目。项目一览中，对重要项目划为○，树形图中测量基准表示为网状。
瞬间停电・停电对策	发生停电或瞬间停电时，为提供安定的电力而制定的对策。
故障时运用	假设系统内部或者相连的外部系统发生故障状态所设计的运用方法。
故障修复	整修制品缺陷。
双重化	正常有一个去掉充分的功能单位，为应对异常而预备复数，使得异常时可以代替运作而预先构成或计划。
信息安全措施方针	表示关于组织安全措施的方针。通常，方针中包括信息安全措施的目标（遵守到什么程度）和组织为达成目标而实施的行动或责任人的明确化等。以这些信息安全措施政策为基础，策定需实施的对策基准，还有实施这些时的顺序。
技能等级	构成信息系统的业务功能或对制品的熟练度。
规模编排	提高服务器处理能力的接近研究对象的一种。并排复数服务器作为系统全体来提高服务器的处理能力。
提高规模	提高服务器处理能力的接近研究对象的一种。或者追加CPU，或者置换成高性能的来提高服务器的处理能力。
网络存储器	构成系统的要素之一，为记忆数据而设的装置。
强压负荷	比通常时的负荷更大的负荷在短时间内显示的现象（超过设想业务量最高点的状态）。尤其像面向一般用户的系统等无法限制客户数的系统中容易发生。
生产能力	系统在每个单位时间里所能处理的工作量。也称为系统处理能力指标。
软弱性	即使实现安全措施对策，也必须考虑的可能性或原因（攻击可能性，运用错误，使用者的不注意，违反规则等）。
功能品质保证	满足功能性需求或者其制定而必须的项目。
安全编程	为了源代码中不含软弱性而实施的程序设计方法。
安全措施	本等级标准中用于安全保护系统信息资产的“信息安全措施”的内容。 广义的“安全措施”包含安全性（对身体或物体无损伤，损害的状态）的内容，但在本等级标准中却不包含。
安全措施统一处理	统一处理中，尤其指的是修正安全措施漏洞的统一处理。

用语	说明
安全措施风险	对于系统或应受保护的资产，不应发生的状态或状况。
安全措施对策	为确保信息安全措施的技术或者用于运用的实现手段。
安全措施风险分析	筛选假想的安全措施风险和安全隐患威胁进行分析。
段分割	根据用途和系统形态分为复数的领域，构成网络。
世代管理	定期取得备份时不仅保管最新数据还保管过去数据，来恢复各自数据的备份管理方式。
选择等级	假想样板系统来选择的等级。由等级值和等级说明所构成。  (关联用语) →基础值
软件分配	把软件故障统一处理及版本上传文件等分配在构成信息系统的机器中。
应答时间	从把要求传送于系统到返回结果的时间。  (关联用语) →回应
宽带保证	宽带是指网络上的速度，对于系统（网络）利用者可保证一定的通信速度。
大规模灾害	因地震，台风等自然现象或暴力行为等的人为破坏行为所造成的灾害。因系统直接受破坏或电力，水道等生活向导无可奈何地被停止，使得系统业务很难继续。
耐故障性	对于故障维持指定的运转水平的能力。故障接受性。
耐震	固定架子等因地震而晃动中保护电脑机器的对策。
代替业务运用	因为故障，系统或是服务的一部分在系统上不可能恢复的情况，使用代替的覆盖这种有可能性的手段。
一重故障	在构成系统要素中，因为双重化要素，发生一部分的故障。一重故障。 因为用其他的代替，所以业务有连续可能的状态。
平常运用	信息系统在所有正常的状态下设想设计的运用方法。
定期维护	定期实施维护作业。有作为消耗品的保全交换的硬件维护与作为磁盘上不要日志的删除软件的维护。
磁盘使用率	保存在磁盘的数据量在全体磁盘容量中使用了多少百分比。 磁盘使用率=（磁盘使用量） / （总磁盘容量）
数据安全性	保证完全的收集全部的数据。保证可以对数据进行正确的操作，对于操作得到期望的品质还有就是可能检查出对数据的变更。数据完整性。
数据恢复	在信息系统中发生故障，恢复所丢失的数据。
符合规格	成品遵循的国际规格、国内规格与海外规格等。
电子签名	为了验证电子文书的合理性而被授权的信息以及使用技术（用电子签名，有可能检查出签名者的特别规定与篡改等。
碎片整理	在数据的记忆领域内发生了空白领域的断片化，用进行数据的重新配置来解决。
电与磁对策	为防止电和磁对系统的影响的对策。
电气设备适合性	对于设置预订场所的电源设备诸元素（电源容量/电压/线路数等）导入机器的适合程度。例如，可以使用100V AC电源、省电对应等机材的情况，一般可以判定为适合程度高。
同一机械材料扩展余力	不是报废已经导入完成的机械材料，根据简单的构成要素的追加、增设等，可以扩展性能与容量。另外，在契约上即使有升级的可能，在箱形交换等必要的情况下，也要判断为当前余力低。
导入支持	在系统中导入成品时，主要支援成品的使用方法、构筑。
二次对应	一次对应后实施的对应。作为二次对应，辨别故障部位，对其部位的故障原因进行追查、修正、确认以及暂时避开策定等。
双重故障	在构成系统的要素中，双重化要素、已经成为单一故障的状态与同要素发生的故障。 发生故障要素有双重化的情况，业务停止。
认证功能	基于识别信息确认用户与机器等的功能。
网络机器	构成系统LAN及与外部连结使用机器。开关、路由器等。
网络诊断	根据对于诊断对象的数据库及网络及其等实施的疑似攻击，诊断其脆弱性。
备份	为了防备丢失数据，保存到不同媒体以可能恢复状态。

用语	说明
批处理应用	进行从统一处理的编排到动作确认的一连串作业（不仅是导入批处理，也含有查证作业）。
高峰时	由于在单位时间里处理量增加等，给系统增加到最大负荷的时候。
拥堵	集中通信与对其处理给予重大影响的多数访问等情况。
附带设备	包含设置服务器的建筑物、电源与支架等，系统附带设备。
恢复作业	故障发生后，恢复到被要求系统水准的作业。
地板设置用机材	单体直接设置在地板面上一样设计的机材。有被称为地板竖型、机柜型、塔型等机材。
同时运作	新系统同现运行系统同时运作的状态。
基础值	同选择等级一样。
别地保管	保管到与备份数据的信息系统场所远距离的地方。
变换规定	在向新系统转移对象数据时，有必要变换的规定。这种变换会根据必要数据量与规定数，其开发与转移的作业量会有很大不同。
保管场所分散度	表示保管外部数据的场所分散至什么程度。
维护员	担当维护运用与故障即时对应的现场作业人员。
维护运用	为了维持系统的正常状态，实施必要作业的运用。  （关联用语） → 平时运用 → 故障时运用
维护部品	为硬件交换部品材料。
恶意软件	计算机病毒、蠕虫、钓鱼软件等有恶意软件的总称。
测量标准	可能客观的测定与计算测量某种事物的具体标准的尺度（指标）。 在非功能性要求等级中，给予各项目等级时，等级指的是可以客观判断的具体指标。
内存使用率	在系统上，OS与应用程序时使用内存的比例。 内存使用率 = （已使用的内存量） / （全部内存量）
减震	减低地震引起的机器摇晃的对策。
处理剩余率	表示可能对应在单位时间想要处理件数的几倍的目标值。（如果设定剩余过大那么就成为过剩投资，如果设定过小的剩余率那么就不能对应假设以外的件数） 平时处理剩余率 = （平时单位时间中处理件数） / （单位时间中处理件数） 高峰时处理剩余率 = （高峰时单位时间中处理件数） / （单位时间中处理件数） 低谷时处理剩余率 = （低谷时单位时间中处理件数） / （单位时间中处理件数）
目标恢复时间	伴随业务停止的故障发生时，对于以RPO与RLO设定的目标值，到恢复为止的需要时间。RTO。实际恢复需要时间的合计值、作为平均恢复时间（MTTR）用来计算运作率的。
目标恢复水准	伴随业务停止的故障发生时，表示恢复到什么程度的目标值与指标。汇总了RTO/RPO/RLO的值。
目标恢复地点	伴随业务停止的故障发生时，设定恢复备份数据将系统恢复到哪个时间点的目标值。RPO。
目标恢复水平	伴随业务停止的故障发生时，恢复到什么水平（只是系统的恢复，还是业务可以立即重新开始的状态）的目标值。
样板系统	参考经济产业省的信赖性指导方针与IPA的重要城市基础设施信息系统信赖性研究会报告书定义非功能性要求项目的系统的范例。范例如下所示。 ・具有极大社会性影响的系统 ・具有局部社会性影响的系统 ・几乎没有社会性影响的系统
样板系统表格	汇总表示每个模板系统的特征的具有代表性的非功能性要求的系统。与等级表一同捆绑。
地板负荷	地板的每平方米设置可能的重量。值越大集中设置大量机器材料的可能性越大。通常的办公室有300Kg/m <sup>2</sup> 的程度，数据中心等也有达到1,000Kg/m <sup>2</sup> 以上的情况。
预兆监视	系统在发生无法挽救的故障前，监视机器轻微的错误与资源使用情况，觉察可能引起麻烦的征兆。可以实施预防维护。  （关联用语） → 预防维护
备用机器	发生故障的服务器与终端的替换用机器。
预防维护	主要是关于消耗品，在发生故障前在规定时间点实施交换。基于使用期间的实施方法与预兆监视的结果的实施方法。  （关联用语） → 预兆监视

【A-Z】

用语	说明
机架式服务器用机材	以19英寸架子等搭载为前提所设计的机材。
资源	CPU/内存/存储器等，为了完善信息系统装置所必要资源的总称。
资源监视	确认关于监视对象的资源“盈亏”状态的监视方法。
远程监视	与存在监视对象场所不同的通知场所监视结果的监视环境实现方式。
远程操作	与信息系统的运行作业或是有维护作业的信息系统场所不同的场所实行运行环境的实现方式。
响应	在系统等从发送要求开始到最初的应答（结果）返回的时间。统一处理的情况是与应答时间（最初的结果返回的时间）相同。  （关联用语） → 应答（时间）
响应遵守率	作为系统目标的达成响应标准的比例（在业务处理中，以全部处理为目标决定的响应，可以完成到哪种程度。）。 响应遵守率 = （满足目标值的全部处理件数） / （全部处理件数）
等级	对于测量标准，把平常取值整理为0-5这6个阶段。但是，不能满足这6个等级阶段时，请参照左面。
等级值	对于每个测量标准定义具体实现等级。0-5的数值与其数值所表示的内容说明构成。
漏电对策	为了防止漏电对系统的损失的对策。有发现对策，切断对策等。  （关联用语） → 切断对策
交替日志	为了防止日志文件的增大，有时以一定期间与一定大小更换日志文件，有时能够删除过去日志的功能。
滚动升级	群构成与双重构成的系统中，活用系切换与低谷运行，每个节点按顺序进行统一处理应用，为了不停止系统的运用，实现统一处理应用的方法。
BtoB (Business to Business)	企业之间的商务模式。交易伙伴多数是固定的事先签约的企业。B2B。
BtoC (Business to Consumer)	通过网络的企业与消费者之间的交易形态。多数情况下的一般消费者是不特定的，所以系统性的需要预测是困难的。B2C。
CO2排出量	提供服务系统排出的CO2的量。不只是用于服务提供中运转的能量消费，还有控制含有机材料的生产与报废等循环的全部排出量。检讨在提倡控制温室效果的京都议定书的排出量交易与碳素税等的附上削减动机。
CPU利用率	在系统上处理OS与应用程序时，使用CPU的比例。正常是表示单位时间内的平均使用率。 CPU使用率 = （在单位时间中使用CPU的时间） / （单位时间）
CSR (Corporate Social Responsibility)	企业的社会责任。具体是指对利害关系者的说明责任、法令遵守及企业管制等活动。自身主动地规定活动，但是与公告与宣传活动等基本上不同。为了能使企业永久的存在与发展，以酿成良好的社会信用为目的。
d B (decibel)	原有的符号是表示无次元的单位，在本文中是作为惯用的噪音声压级的单位来使用的（正确的是、dB SPL）。采取对数表现的手法，即6dB约2倍、10dB约3倍的声压的意思，例如，60dB约是50dB的3倍声压的意思。
DB诊断 (DataBase诊断)	对于诊断对象的数据库，假设来自系统内部与外部的攻击，分析是否不存在易于破坏的设置等。
DR (Disaster Recovery )	发生不可预期的灾害与故障等，对系统有很大影响时，为了恢复业务的手段或计划。
DR site	由于大规模灾害不可能恢复正常运行系统的情况，设置可以代替系统的网站。
IHV (Independent Hardware Vendor)	进入不到特定的硬件制造商的控制下，制造与销售固有硬件的硬件企业。
ISV (Independent Software Vendor)	进入不到特定软件制造商的控制下，制造与销售固有软件的软件企业。
MTBF (Mean Time Between Failure)	系统发生故障开始到下一个故障发生的平均间隔（时间）。平均故障间隔。用运作时间（运行时间）的合计值除以发生故障次数所得的值表示。

用语	说明
MTTR (Mean Time To Repair/ Mean Time To Recover)	系统中从发生故障到恢复为止的平均时间。表现为系统的恢复时间的合计值除以发生故障次数的值。
RAID (Redundant Arrays of Independent(Inexpensive) Disks)	组合多个硬盘，提高可信度并实现高速化的技术。包括RAID1的镜像化和错误修改符号分散到多个硬盘中提高可信度的RAID5等。
RLO (Recovery Level Objective)	伴随业务停止而发生故障时的恢复水平目标值。即目标恢复水平。
RoHS指令 (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment)	欧洲联合（EC）指定的关于限制使用含有有害物质的电器电子设备的规定。该规定考虑到处理含有有害物质的电器电子设备对环境的影响。规定了六种物质（铅，汞，铬，六价铬，多溴联苯，多溴二苯醚等）的最大浓度。该规定适用于所有欧盟上市的电器电子设备。
RoSPA (The Royal Society for the Prevention of Accidents)	英国国立灾害防止协会。规定了防止劳动灾害的噪音基准等。
RPO (Recovery Point Objective)	伴随业务停止而发生故障时，确定由备份数据将系统恢复到哪个时点的目标值。即目标恢复地点。
RT0 (Recovery Time Objective)	伴随业务停止而发生故障时，恢复到RPO及RLO所设定的目标值所需要的目标时间。即目标恢复时间。 实际恢复所需合计时间作为平均恢复时间（MTTR）用于计算运转率。 相关用语 →RPO →RLO →MTTR
Sorry动作	当系统高负荷运行时，不仅是系统无响应，而且是向使用者提供“系统繁忙”等状态报告并提供应急方案说明。不设置Sorry动作时，系统一般为无响应状态。
SPOF (Single Point of Failure)	当个别部位发生故障时，停止系统的组件。即单一故障点。
UL60950	世界著名IT设备的产品安全规格。由美国独立系统的安全规格开发机构，检测・认证机关颁布。Underwriters Laboratories Inc.（略称：UL）
VCCI (Voluntary Control Council for Interference by Information Technology Equipment)	针对由于个人电脑，传真等信息技术装置导致收音机、电视机等接收器的信号故障谋求解决方案的国内行业独立规定团体，即“信息处理装置等信号故障自主规定协会”的简称。
WAF (Web Application Firewall)	对于Web服务器与Web应用程序遭到攻击，检测接受数据，及防止破坏的防火墙。
Web诊断	对于网站运行的Web服务器与Web应用程序的安全措施诊断。



## 5 附录

### 5.1 与有关非功能性要求其他活动的关系

除了非功能性要求等级，还有关于“非功能性要求”的标准与指导方针。为了能够明确非功能性要求等级与其他活动的差的非功能性要求等级的定位，以设定利用工程来表示与其他指导方针的关系为主，如下图所示。

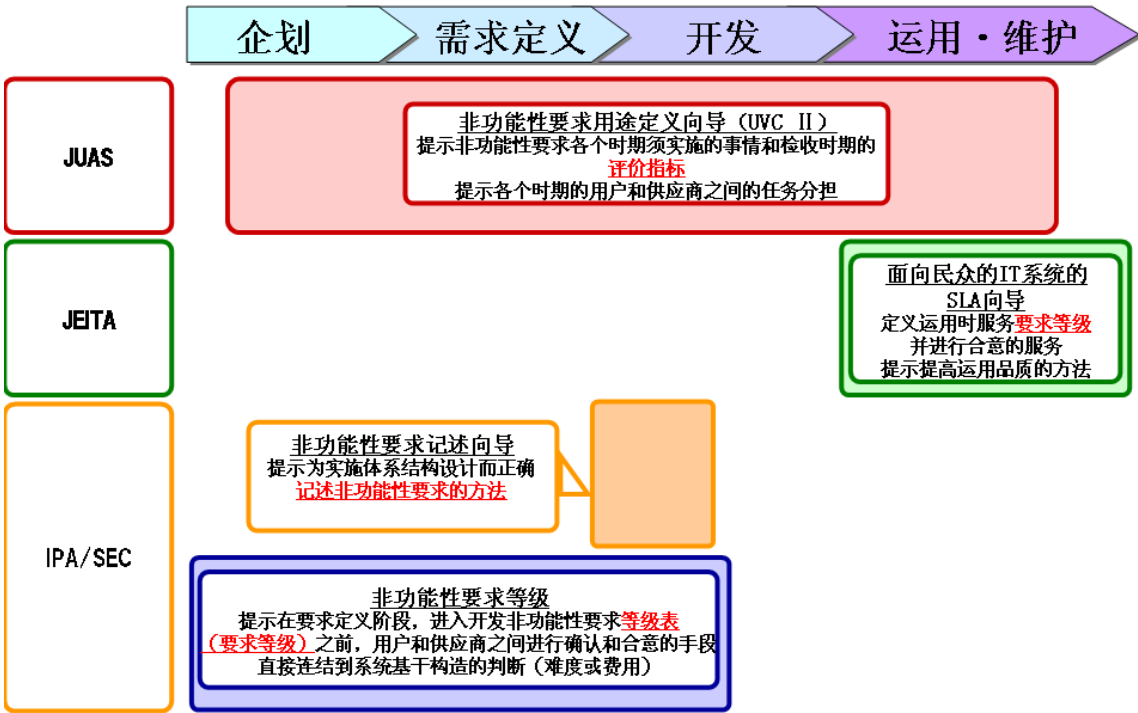


图 5.1.1 假设使用工程与各种标准活动

非功能性要求等级是指，在用户与供应商之间确认合意作为主要的上游工程的要求项目与其要求等级为目标，可以与其他目标的其他指导方针共同使用。以下表示的是与其他指导方针的关系。

#### 5.1.1 与 JUAS “非功能性要求方法定义指导方针 2008” 的关系

“非功能性要求方法定义指导方针 2008（以下、UVC II）”是指，社团法人 日本信息系统与用户协会（JUAS）所策定的指导方针，以系统发包方的角度来进行关于系统整体的非功能性要求，在承包方验收系统时，必须验证的非功能性要求项目的整理。具体来说，表示上游工程到下游工程的各阶段的要求定义的方法，特别是表示可能测定的要求定义项目的制定方法，表示其验证要点，并在这个点上有自己的特征。另外，使用整理的非功能性要求项目分为广泛的、功能性、信赖性、使用性、效率性、维护性、转移性、控制故障性、效果性、运行性及技术要件等十个分类。

UVC II 与非功能性要求等级，在使用非功能性要求项目的范围上有差距。非功能性要求等级，为了判断系统基础而把非功能性要求作为检讨范围，在每个要求项目中表示系统基础的每个构筑难度的要求等级。因此，即使在 UVC II 分类中，功能性、实用性、转移性等，与系统基础的判断没有直接关系的项目，大部分作为范围外的这一点上有所不同。

使用两者的情况下，从上游开始直到验收为止定义的系统全部的非功能性要求，可以采用 UVC II。但是特别是在上游确认并合意具体的系统基础必须具备的非功能性要求时，采用“非功能性要求等级”更有效果。

### 5.1.2 与 JEITA “面向民众 IT 系统的 SLA 指导方针” 的关系

依据社团法人 电子信息产业协会（JEITA），已经改定完第三版的“面向民众 IT 系统的 SLA 指导方针”是，作为根据信息系统所提供的评价 IT 服务品质的指标，SLA 及采用 SLA 提高 IT 服务的运行等级为目标的思考方式。另外，在 2009 年 3 月发行的“关于 SLA 应用领域扩大的调查报告书”中，表示系统开发的 SLA 及开发与运行紧密联合的指标。

非功能性要求等级是，主要作为开发时的判断来表示要求等级，与表示运行时的服务等级的 SLA 在使用时机上是不同的。在使用两者的情况下，要考虑到利用各种各样的时机，调合开发契约与运行契约场面不同。

### 5.1.3 与 IPA/SEC “非功能性要求记述向导” 的关系

据信息处理推进机构软件工程中心（IPA/SEC）2008 年 7 月总结的“非功能性要求记述向导”，为了提示效率性且网罗性地记述因系统的体系结构设计而正确充分的非功能性要求的方法，所以决定了记述项目模板化等的记述规则。

定义非功能性要求的人可以利用非功能性要求等级，首先在企划・需求定义时确认要求等级，参考“非功能性要求记述向导”，可利用要件定义更为详细地记述。

## 5.2 与其他活动的关系

非功能性要求等级根据制定有时参考“沿袭想法”、“引用”、“配合用语”等标准规格。还有，在非功能性要求等级中，单单关于非功能要求，可以在用户与供应商的之间进行合意。但是，另外存在其他应遵守的规程等时，需要配合那些规程来进行探讨。以下，介绍与那些其他标准的关系。

### 5.2.1 与 ISO/IEC 9126-1:2001 的关系

有关非功能性要求的代表性标准有“ISO/IEC 9126-1:2001 (JIS X0129-1:2003)<sup>1</sup>”(以下简称 ISO/IEC 9126)。ISO/IEC 9126 是指以软件为对象，从外部品质和内部品质两方面定义品质特性的国际标准规格。

与以系统基础的非功能性要求为对象，非功能性要求等级无法一概地比较，但用语在可能的范围之内可参考 ISO/IEC 9126。假设定义软件品质特性的 ISO/IEC 9126 解释为定义系统基础的品质特性而相比较的话，与非功能性要求等级各大项的对应关系如表 5.2.1.1 所示。

观察这个表的对应关系的话，ISO/IEC 9126 的品质副特性和非功能性要求等级的大项之间存在无对应关系的部分。无对应关系的理由为在 1.3 节所表示的范围一样，非功能性要求等级是以对系统基础的发包方的要求“可视化”为目的，所以对于表示只由软件作成的应用程序品质的部分，不视为探讨对象。比如，如“使用性”，在软件中是以应用程序的性质而存在，却不以系统基础的性质而存在。

---

<sup>1</sup> 2009 年 12 月现在、ISO/IEC 9126 的后继规格的 SQuaRE(被称为 Software Product Quality Requirements and Evaluation) ISO/IEC 25000 系列在整备中。全部的指导 ISO/IEC 25000:2005 的其他、发行的 ISO/IEC 25030:2007 Quality Requirements 等。



表 5.2.1.1 与 ISO/IEC 9126 非功能性要求等级的对应关系

特性	定义	品质副特性	定义	对应大项
功能性	软件在被指定的条件下使用时，提供符合明示性暗示性的必要性功能的软件产品能力	合目的性	提供给与指定作业及使用者的具体目标相对应的功能集合的软件产品能力	—
		正确性	在必要的精确度下，拥有正确的结果或是正确的效果；还有被允许的结果或是被允许的效果的软件产品能力	—
		相互运用性	与一个以上指定系统相互作用的软件产品能力	—
		安全措施	为了没被许可的人或系统不可读取或者修正信息和数据，及被认可的人或系统访问信息和数据时不被拒绝，而保护信息和数据的软件产品能力	安全措施
		功能性标准适合性	遵循与功能性相关联的规格、规约；法律上的以及类似的法规上的规则软件产品能力	安全措施、系统环境·低碳环保
信赖性	在指定条件下使用时维护被指定的完成标准的软件产品能力	成熟性	回避软件潜在故障发生的软件产品能力	可用性
		故障容忍性	在实施了软件的故障部分时又或者违反了被规格化的接口的情况发生时，维持指定的达成标准的软件产品能力	可用性
		恢复性	故障发生时，对指定的达成标准进行再确立，恢复受直接影响的数据的软件产品能力	可用性、运用·维护性
		信赖性标准适合性	遵守与信赖性相关联的规格、规约以及规则的软件产品能力	系统环境·低碳环保
使用性	在指定的条件下使用时可以理解、学习、利用，对于使用者而言有吸引力的软件产品能力	理解性	软件在特定作业中，是否适用特定的使用条件，以及怎样使用可以使用者得以理解的软件产品能力	—
		学习性	使用者能够学习到软件的使用性的软件产品能力	运用·维护性
		运用性	使用者可以进行软件的运用以及运用管理的软件产品能力	运用·维护性
		魅力性	对使用者有魅力性的软件产品能力	—
		使用性标准适合性	遵守与使用性相关联的规格、规约、标题向导以及规则的软件产品能力	系统环境·低碳环保
效率性	在明示的条件下对比使用的资源量提供适合性功能的软件产品能力	时间效率性	在明示的条件下实施软件的功能时，提供贴切的应答时间、处理时间以及处理能力的软件产品能力	性能·扩展性
		资源效率性	在明示条件下实施软件的功能时，正确的使用资源量和资源种类的软件产品能力	性能·扩展性
		效率性标准适合性	遵守与效率性相关的规格与规约的软件产品能力	性能·扩展性、系统环境·低碳环保
维护性	与修正的简易程度有关的软件产品能力	解析性	软件缺陷的诊断与故障原因的追查、以及软件修改场所的识别的软件产品能力	运用·维护性
		变更性	执行指定修改的软件产品能力	—
		安定性	避免因软件修改所引起的无法预期的影响的软件产品能力	—
		试验性	确认修改的软件的妥当性的软件产品的能力	—
		维护性标准适合性	遵守与维护性有关的规格与规约的软件产品能力	性能·扩展性、系统环境·低碳环保
移植性	从一个环境置换到另外一个环境的软件产品能力	环境适用性	在预先准备好以外的附加作业或者无手段被指定的不同环境中，适用软件的软件产品能力	移行性
		设置性	为了设置与指定环境的软件产品能力	系统环境·低碳环保
		共存性	在拥有共同资源的共同环境中，与其他独立软件共存的软件产品能力	可转移性
		置换性	在相同的环境下，为了同样的目的，可以从其他指定的软件产品中置换而来使用的软件产品能力	可转移性
		移植性标准适合性	遵守与移植性相关联的规格、规约的软件产品能力	系统环境·低碳环保

### 5.2.2 与标准框架 2007 的关系

标准框架 2007 是指，向发承包方提供与系统构筑有关的相关作业项目的标准框架。从系统的构想到废弃为止所必须的作业项目及其作用不依存于作业工程、开发模型与开发技法/工具，作为产业界的共识进行的概括性的规定。另外，软件、运作周期、程序（SLCP-JCF2007）的国际规格 ISO/IEC 12207:2007（JIS X 0160）作为基础，包括以软件为中心的系统的联合作业，特别是在上游工程等日本独自地强化并扩张。

非功能性要求等级，这个标准框架 2007 作为业界的系统构筑作业与程序的标准规格，参考了被规定的项目与角色分担。

### 5.2.3 与关于增强信息系统的信赖性指导方针的关系

有关增强信息系统的信赖性指导方针（信赖性指导方针）是指，因信息系统损害对社会产生的影响逐渐加深，经济产业省在 2006 年第 1 版、2009 年 3 月第 2 版中制作的指导方针。以这个制作目的为背景，在非功能性要求中，特别着眼于信赖性、安全性，以提高其水平为目的。此指导方针为了提升信赖性每个种类的发承包方的开发时间、运行时间、损害发生时间的实施项目，或是技术性的注意事项都要进行表示。

在非功能性要求等级中，列示了与此信赖性指导方针的关联政策——“重要基础信息系统信赖性研究会”所表示出的系统文件的名称，把 3 个样板系统进行再定义。此外，非功能性要求等级自身也是要通过增强信赖性的政策的需求定义所表示的“通用共识支援工具”来进行协调与讨论，最终把信赖性指导方针定位于其他政策的中心。

### 5.2.4 与 ISO/IEC 15408 (Common Criteria)的关系

ISO/IEC 15408:1999 是规定了信息系统与其构成的机器、软件的安全措施评价基准的国际标准规格。由 3 部分组成，发行了 ISO/IEC15408-1:2005、ISO/IEC15408-2:2008、ISO/IEC15408-3:2005 3 个规格。非功能性要求等级中，与系统的安全措施相关的基本概念与用语，沿袭了 ISO/IEC15408 的内容。

ISO/IEC 15408 是由欧美 6 国组成的 CC 项目开发而成的，是被称为 Common Criteria 的国际标准化的评价标准，以 ISO/IEC 15408 为基础的“IT 安全措施评价及认证制度”在国际间（包括日本）被广泛的应用。在日本国内，以 ISO/IEC 15408 为基础的评价认证制度主要活用与政府机关的系统调査<sup>2</sup>中。如下例所示。

#### ① 对应系统的特定构成要素的运用案例

有针对构成系统的保护产品，以 ISO/IEC 15408 为准的评价与认证的取得被作为要求事项的案例。特别适用于 IC 卡、密码产品、防火墙等需要高度保护的系统构成要素。

---

<sup>2</sup> 参照《灵活运用 ISO/IEC15408 的向导书（经济产业省 商务信息政策局 信息安全措施室）》

② 需要 ISO/IEC 15408 为准的安全措施设计规格书的案例

ISO/IEC 15408 中被称为 ST (Security Target) 的定义为安全措施设计规格书被定义，开发对象的系统要求高保护的时候，需要以 ISO/IEC 15408 为准的“安全措施设计规格书”的制作与第三者评价机关的内容的妥当性进行评价。

这些都被列举为系统所要求的事项，由于会影响系统开发的成本，需要重新确认是否相对应。

### 5.2.5 与 ISO/IEC 27000 系列的关系

ISO/IEC 27000 系列是指，为了确保与维持信息保护，在组织内实施的与体系化、系统化相关的 ISMS 的国际标准规格。

2009 年 12 月末时，发行了 ISO/IEC 27001:2005(要求事项)与 ISO/IEC 27002:2005(实践的规范)<sup>3</sup>。在日本国内，进行了 ISO/IEC 27001 的适应性的评价与认定，运行了“ISMS 适应性评价制度”，在企业及组织内部进行了广泛的普及。

ISMS 不仅仅是一个系统，以运用此系统的组织作为对象，规定了技术上的、物理上的、人力上的、组织上的各个管理政策，使经营层作为顶点，有组织性的进行实施。非功能性要求等级中，以系统的要求导出作为范围，系统的利用、运用面的物理上的、人力上的、组织上的保护要求被导出时，在 ISO/IEC27002 中具体的管理政策会被显示为最好的练习，并可以加以参考。

另外，取得了 ISMS 认证（或是即将取得认证）的组织内的运用系统的保护要求的导出时，需要用 ISMS 达到与已被测定的技术上的管理对策的整合。这主要与项目一览的中间项目“访问、使用限制”、“异常的追踪与监视”、“网络对策”相对应。

### 5.2.6 与政府机关的信息安全对策的统一标准的关系

政府机关的信息安全对策的统一标准（政府统一标准）是国内政府机关（各府省厅）的信息安全对策的基准。构筑政府机关的系统时，以遵照政府统一标准为义务、必须严格的确认被导出的安全要求的结果是否遵照政府统一标准。

在政府统一标准中，把应进行实施的安全对策分为“基本”（必须实施的对策）、“强化”（可选的实施对策），没有把所有安全对策都设定为必须实施的对策。为此，面向政府机关的系统在使用非功能性要求等级时应遵循政府统一标准所实施的必须的安全对策，除必须实施的以外的安全程序，要参考非功能性要求等级所导出的要求的使用方法。

另外，政府统一标准规定的信息安全对策，包含了广泛的安全性，包括系统面对灾害与故障时的“可用性”，和为了维持此“可用性”的“运用、维护性”。在进行“可用性”与“运用、维护性”要求的讨论时，有必要确认政府统一标准与其的整合性。

---

<sup>3</sup> 截至目前 2009 年 12 月 ISO/IEC 27000 系列仍在完善中，除此以外、ISO/IEC 27005:2008（信息安全风险管理），ISO/IEC 27006:2007（检查及认证机关的要求事项）等已发行。

### 5.2.7 与金融机关等计算机系统的安全对策标准的关系

金融机关等计算机系统的安全对策标准（FISC 安全对策基准）是金融信息系统中心（FISC）所规定的，国内金融机关安全对策的标准。通常，在构建金融机关的系统时，为了把 FISC 安全对策标准的依据作为调配的条件，在安全要求导出时，结果需要确认是否以 FISC 安全对策标准为依据。

FISC 安全对策标准与政府统一标准同样，把它应该实施的安全对策分为必须项目与任意项目两种。在金融机关系统中使用非功能性要求等级时，遵从用 FISC 安全对策基准所必须的安全政策，必须以外的安全对策，参照非功能性要求等级，可以导出要求等的使用方法。

另外，FISC 安全对策标准中所定义的对策是金融系统性质上的、与系统的灾害、故障相对的“可用性”、运用设施等与“系统环境、低碳环保”相关的对策也包含在此，讨论“可用性”与“系统环境、低碳保护”时，要确认与 FISC 安全对策标准的整合性。

### 5.2.8 与 Payment Card Industry Data Security Standard 的关系

Payment Card Industry Data Security Standard（PCI DSS）是信用产业规定的国际性的安全基准，以信用卡的加盟店与代办结算者所持有的信用卡信息的安全作为对象。

在信用卡加盟店等的信用卡信息持有系统中，使 PCI DSS 成为必要依据，与之相对应的系统的安全要求被导出时，他的结果需要以 PCI DSS 的基准相对应进行充分的确认。

在适用 PCI DSS 的系统中使用非功能性要求等级时，首先要遵循 PCI DSS 所显示的要求，PCI DSS 中没有明确显示的项目参考非功能性要求等级，也能导出要求的使用方法。

### 5.3 参考文献

- [1] 独立行政法人 信息处理推进机构软件工程中心 (IPA/SEC), 《标准框架 2007 ～经营者、业务部门参与企划的系统开发及交易用》, 欧姆社, 2007 年 10 月 1 日
- [2] 独立行政法人 信息处理推进机构软件工程中心 (IPA/SEC), 《经营者参与企划的要求品质的确保 ～从超上游主攻的 IT 化第 2 版》, 欧姆社, 2006 年 5 月 25 日
- [3] 经济产业省 软件开发力强化推进临时小组 要求工学・设计开发技术研究会 非功能性要求与构架 WG, 《非功能性要求记述向导》,  
[http://sec.ipa.go.jp/reports/20080717/NFRdescription\\_guideline.pdf](http://sec.ipa.go.jp/reports/20080717/NFRdescription_guideline.pdf),  
2008 年 7 月
- [4] 社团法人 日本信息系统使用协会 (JUAS), 《非功能要求规格定义指导方针 2008》, 2008 年 7 月
- [5] 社团法人 电子信息产业协会 (JEITA) 解决服务事业委员会,  
《面向民间 IT 系统的 SLA 指导方针 第三版》, 日经 BP 社, 2006 年 10 月 2 日
- [6] 社团法人 电子信息产业协会 (JEITA) 解决服务事业委员会,  
《与 SLA 适用领域的扩大有关的调查报告书》, 社团法人 电子信息产业协会,  
2009 年 3 月
- [7] 经济产业省, 《与提高信息系统的信赖性有关的指导方针》,  
<http://www.meti.go.jp/press/20060615002/20060615002.html>, 2006 年 6 月 15 日
- [8] 经济产业省, 『与提高信息系统的信赖性有关的指导方针 第 2 版』,  
<http://www.meti.go.jp/press/20090324004/20090324004-4.pdf>, 2009 年 3 月 24 日
- [9] 经济产业省 商务信息政策局 信息保护政策室,  
《活用 ISO/IEC 15408 供给的向导》,  
[http://www.meti.go.jp/policy/netsecurity/downloadfiles/CCguide\\_ver2\\_0.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/CCguide_ver2_0.pdf),  
2004 年 8 月 11 日
- [10] 内阁官方信息保护中心 (NISC), 《政府机关的信息保护对策的统一标准》,  
<http://www.nisc.go.jp/active/general/kijun01.html>,  
2009 年 2 月 3 日
- [11] 金融信息系统中心 (FISC), 《金融机关等计算机中心的安全对策基准及解说书 (第 7 版)》, 金融信息系统中心 (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) 数据安全措施基准 - 要件与安全措施评估手順版本 1.2》,   
[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml),  
2008 年 10 月
- [19]独立行政法人 信息处理推进机构软件工程中心 (IPA/SEC), 重要城市基础设施信息系统信赖性研究会报告书,   
<http://sec.ipa.go.jp/reports/20090409.html>, 2009 年 4 月
- [20]经济产业省, 非功能性要求等级“用户观点检讨委员会”报告书,   
[http://www.meti.go.jp/policy/it\\_policy/softseibi/hikinou\\_grade.pdf](http://www.meti.go.jp/policy/it_policy/softseibi/hikinou_grade.pdf), 2009 年 6 月