平成２５年度
研究開発事業

地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究

平成２６年３月

財団法人　地方自治情報センター

はじめに

地方自治情報センターの研究開発事業は、地方公共団体が共通的に利用できる情報システム及び新技術の導入並びに新分野へのコンピュータ利用等に関して、研究・開発及び調査等を実施し、地方公共団体の ICT 化等電子自治体の推進等に資することを目的に実施しております。

本調査研究では、地方公共団体の情報システムが備えるべき可用性、性能・拡張性、運用保守性についての非機能要件が機能要件と並んで重要なものであることにも拘わらず、一部の地方公共団体を除いて十分認識されておらず、情報システム調達仕様書に必要な事項があまり示されていない実態に鑑み、地方公共団体の情報システムの安定的な稼働を推進するため、地方公共団体の情報システム調達仕様書における非機能要件の標準化に取り組むこととしました。

この非機能要件の標準化に当たっては、独立行政法人情報処理推進機構にご協力いただき、当該機構が作成した「非機能要求グレード」を参考として、地方公共団体において調達時により利用しやすくなるように、地方公共団体の特性を考慮した非機能要求グレード（地方公共団体版）を作成しました。

この「非機能要求グレード（地方公共団体版）」を、地方公共団体の皆様に御活用いただければ幸いと存じます。

本調査研究の実施に当たり、適切な御指導・御助言をいただいた本調査研究委員会の委員及び WG メンバーの皆様、ヒアリング調査等にご協力いただきました地方公共団体の皆様に、厚く御礼申し上げます。

平成２６年３月

財団法人 地方自治情報センター
理事長　　戸 田　夏 生

目　　次

―　調　査　研　究　報　告　書　―

第１章　調査研究の概要 1
　第１節　背景及び目的 1
　第２節　実施内容 4
　　１　調査研究の全体の流れ 4
　第３節　実施体制 5
　　１　実施体制 5
　　２　調査研究委員会及び WG 5
第２章　地方公共団体の情報システム調達仕様書における非機能要件の現状と課題 7
　第１節　非機能要件に関する現状 7
　　１　調査の概要 7
　　２　地方公共団体における情報システム調達仕様書の実態 7
　　３　地方公共団体における非機能要件の定義方法 8
　　４　地方公共団体の特性 10
　第２節　非機能要件に関する課題 11
　　１　非機能要件という概念の浸透 11
　　２　適切な非機能要件の定義ができる手法の確立 11
　　３　発注者と受注者の合意と非機能要件の標準化 11
　　４　地方公共団体の特性を考慮した非機能要件の標準化 11
　　５　情報システムの調達における職員負担の軽減 11
第３章　非機能要件の標準化の動向 13
　第１節　非機能要求グレードの取組の概要 13
　　１　非機能要求グレードとは 13
　　２　非機能要求グレードの特徴 13
　　３　非機能要求グレードの利用効果 15
第４章　非機能要求グレード（地方公共団体版）について 17
　第１節　基本的な考え方 17
　　１　本調査研究の対象範囲 17
　　２　対象とする非機能要件の範囲 18
　　３　地方公共団体版で考慮すべき事項 20
　　４　非機能要求グレード（地方公共団体版）の構成 21

５　IPA の非機能要求グレードとの関係 22
第２節　活用シートの地方公共団体への適用における考え方 24
１　活用シートの構成の考え方 24
２　活用シートの要件項目（メトリクス）の考え方 25
３　活用シートの掲載項目等 31
第３節　業務・情報システムの分類の考え方 34
１　分類軸の設定 34
２　レベル設定の考え方 38
３　業務システムの分類 43
第５章　今後の展望と課題 46
第１節　環境変化への対応 46
第２節　非機能要求グレードの普及促進 46
第３節　情報システム調達手法全体の標準化 47

― 利　用　ガ　イ　ド ―

第１章　非機能要求グレード（地方公共団体版）の概要 1
第１節　はじめに 1
１　情報システム調達仕様書における非機能要件の定義の困難性 1
２　非機能要求グレード（地方公共団体版）の考え方 2
３　非機能要求グレード（地方公共団体版）利用のメリット 4
第２節　非機能要求グレード（地方公共団体版）の構成 5
第２章　非機能要求グレード（地方公共団体版）の対象 6
第１節　利用者 6
第２節　利用工程 7
第３節　適用対象 8
１　情報システム調達仕様書における範囲 8
２　調達対象と非機能要件における範囲 8
３　クラウドに対する適用 10
第３章　非機能要求グレード（地方公共団体版）の利用方法 12
第１節　活用シートの構成 12
第２節　活用シートの項目 14
第３節　利用手順 16
第４節　準備作業と全庁的要求事項シートの作成 17

１　活用シートの記載内容の調整（必要に応じて実施）　【主な実施者：ICT 部門】..... 17
２　全庁的要求事項シートのレベル調整　【主な実施者：ICT 部門】 17
３　庁内の利用環境の整備　【主な実施者：ICT 部門】 18
第５節　調達案件に応じたシートの検討..... 19
１　業務・情報システムグループの選択　【主な実施者：業務主管部門】 19
２　項目の取捨選択　【主な実施者：業務主管部門】 21
第６節　業務主管部門要求事項シートの作成 22
１　業務主管部門要求事項シートのレベル調整 22
第７節　実現方法要求事項シートの作成..... 24
１　RFI 等の実施　　【主な実施者：ICT 部門若しくは業務主管部門】..... 24
２　実現方法要求事項シートのレベル調整　【主な実施者：ICT 部門若しくは業務主管部門】..... 25
第８節　検討結果の情報システム調達仕様書への反映..... 26
１　非機能要件の確定　【主な実施者：業務主管部門】 26
２　検討結果の情報システム調達仕様書への反映　【主な実施者：業務主管部門】..... 26
第４章　レベル調整時の留意点..... 29
第１節　全庁的要求事項シート 29
第２節　業務主管部門要求事項シート 35
第３節　実現方法要求事項シート..... 47
用語集 54
参考資料　IPA の非機能要求グレードとの関係..... 59

― 項　目　一　覧 ―

項目一覧 1

― 活　用　シ　ー　ト ―

業務・情報システムグループ①..... 1
業務・情報システムグループ②..... 1
業務・情報システムグループ③..... 1
業務・情報システムグループ④..... 1

地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究
報告書

平成 26 年 3 月

財団法人　地方自治情報センター

目次

第１章　調査研究の概要 1
　第１節　背景及び目的 1
　第２節　実施内容 4
　　１　調査研究の全体の流れ 4
　第３節　実施体制 5
　　１　実施体制 5
　　２　調査研究委員会及び WG 5
第２章　地方公共団体の情報システム調達仕様書における非機能要件の現状と課題 7
　第１節　非機能要件に関する現状 7
　　１　調査の概要 7
　　２　地方公共団体における情報システム調達仕様書の実態 7
　　３　地方公共団体における非機能要件の定義方法 8
　　４　地方公共団体の特性 10
　第２節　非機能要件に関する課題 11
　　１　非機能要件という概念の浸透 11
　　２　適切な非機能要件の定義ができる手法の確立 11
　　３　発注者と受注者の合意と非機能要件の標準化 11
　　４　地方公共団体の特性を考慮した非機能要件の標準化 11
　　５　情報システムの調達における職員負担の軽減 11
第３章　非機能要件の標準化の動向 13
　第１節　非機能要求グレードの取組の概要 13
　　１　非機能要求グレードとは 13
　　２　非機能要求グレードの特徴 13
　　３　非機能要求グレードの利用効果 15
第４章　非機能要求グレード（地方公共団体版）について 17
　第１節　基本的な考え方 17
　　１　本調査研究の対象範囲 17
　　２　対象とする非機能要件の範囲 18
　　３　地方公共団体版で考慮すべき事項 20
　　４　非機能要求グレード（地方公共団体版）の構成 21
　　５　IPA の非機能要求グレードとの関係 22
　第２節　活用シートの地方公共団体への適用における考え方 24
　　１　活用シートの構成の考え方 24
　　２　活用シートの要件項目（メトリクス）の考え方 25

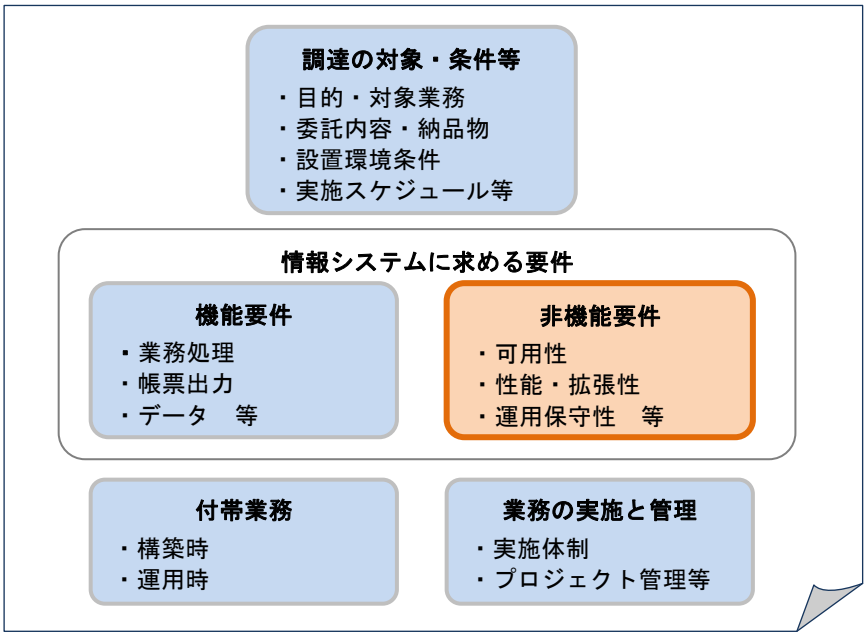
３　活用シートの掲載項目等 31
第３節　業務・情報システムの分類の考え方 34
１　分類軸の設定 34
２　レベル設定の考え方 38
３　業務システムの分類 43
第５章　今後の展望と課題 46
第１節　環境変化への対応 46
第２節　非機能要求グレードの普及促進 46
第３節　情報システム調達手法全体の標準化 47

第１章 調査研究の概要

第１節 背景及び目的

情報システムを調達するに当たっては、どのような情報システムを求めるか要件を明確にする必要があり、その内容を情報システム調達仕様書として表す必要がある。

情報システム調達仕様書に表す内容としては、大きく分けると、図－1 に示すとおり情報システムに求める要件（機能要件、非機能要件）を記載する部分のほか、調達の対象や条件、付帯業務等を記載する部分がある。



図－１　情報システム調達仕様書の要素（項目は例）

機能要件とは、例えばどのような情報を入力し、どのような処理を行い、結果どのような出力がされるか、といった業務の実現のために情報システムが提供する機能に関する要件である。例えば、「住民の異動情報を登録・管理したい」「証明書を発行したい」といったものがそれに当たる。具体的な業務処理に関係するため、地方公共団体職員においても比較的理解しやすい。

非機能要件とは、図－1 の「情報システムに求めるの要件」のうち、文字どおり、この「機能要件」に関するもの以外の要件を指す。例えば、以下のような情報システムの構成や機器の数量等の根拠になるなど情報システムのコスト等に直結するものであり、情報システムを適切に調達するために、機能要件と同等以上に重要な要件である。

○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）

・運用スケジュール（稼働時・停止予定など）

・障害・災害時における稼働目標

○性能・拡張性（情報システムの性能及び将来のシステム拡張に関する要求）

・業務量及び今後の増加の見積り

・情報システム化対象業務の特性（ピーク時、通常時、縮退時など）

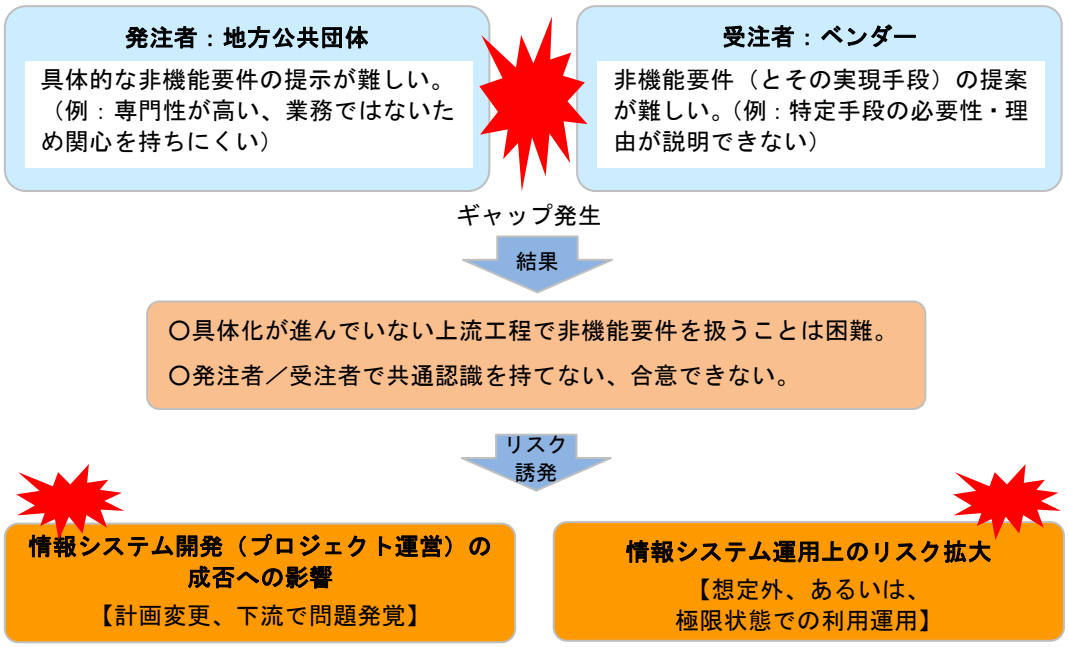
○運用・保守性（情報システムの運用と保守サービスに関する要求）

・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　等

しかし、非機能要件は、後述する調査結果に示したように、地方公共団体の情報システム調達において十分に認識されていない。加えて、業務との関係が見えにくい抽象的なものが多く、技術的な内容を含むものが多いことから、機能要件に比べてどのような項目を定めるべきなのか、どの程度の要件にすべきかを決めることが難しい状況となっている。一方、ベンダー側においても、非機能要件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しにくい状況となっている。

この結果、発注者側である地方公共団体と受注者側であるベンダー間でギャップが生じ、開発や運用段階になって、トラブルが発生する大きな要因となるおそれがある（図－2）。情報システムの適切な開発、安定的な運用を図るためには、そのギャップを解消し、適切に非機能要件を定義することが重要である。



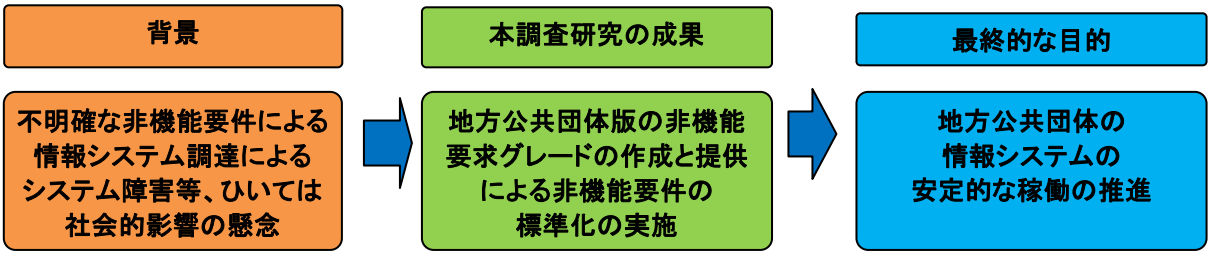
出所：IPA「非機能要求グレード利用ガイド［解説編］」2010 年 4 月を基に作成

図－ 2　非機能要件における問題点

また、地方公共団体で利用する情報システムは共通性が多く、民間の情報システムと比べると要件の標準化がしやすいという特徴があり、適用した場合の効果が期待できる。そのため、当センターは情報システムの調達時に地方公共団体の情報システムが備えるべき非機能要件とそのレベル設定等の技法の標準化を実施することにより、地方公共団体の情報システムの安定的な稼働を推進することを目的に調査研究することとした。（図－3）

上記に当たり、非機能要件については、独立行政法人情報処理推進機構（以下「IPA」

という。）から、一般向けに非機能要件を分かりやすく決定、表現することのできる充実した資料として「非機能要求グレード」が提供されていたことから、本調査研究は、より地方公共団体で利用しやすくなるように、非機能要求グレード（地方公共団体版）を作成する。

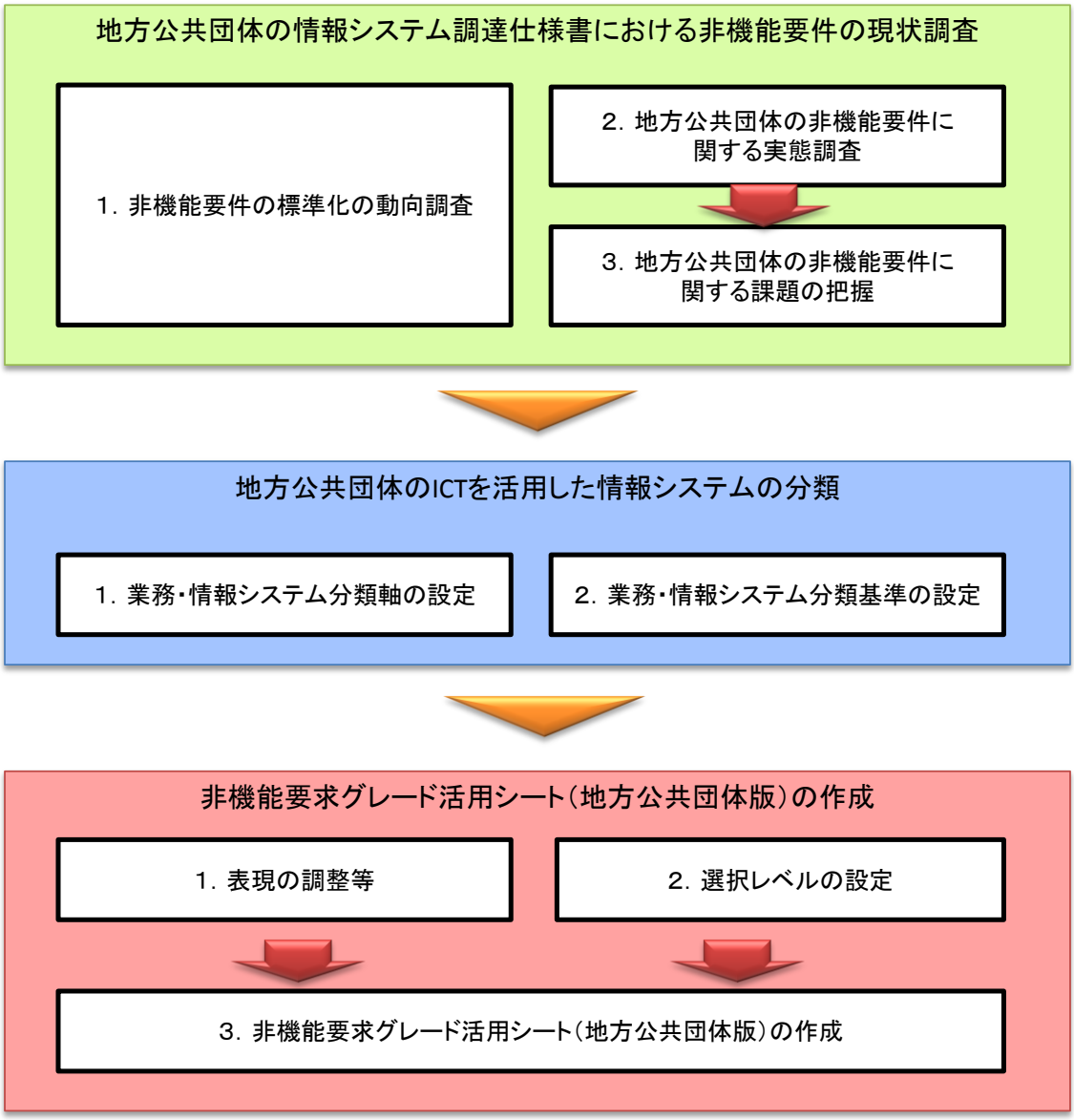


図－3　本調査研究の背景と目的

第２節 実施内容

１　調査研究の全体の流れ

本調査研究は、図－４に示す流れで実施した。

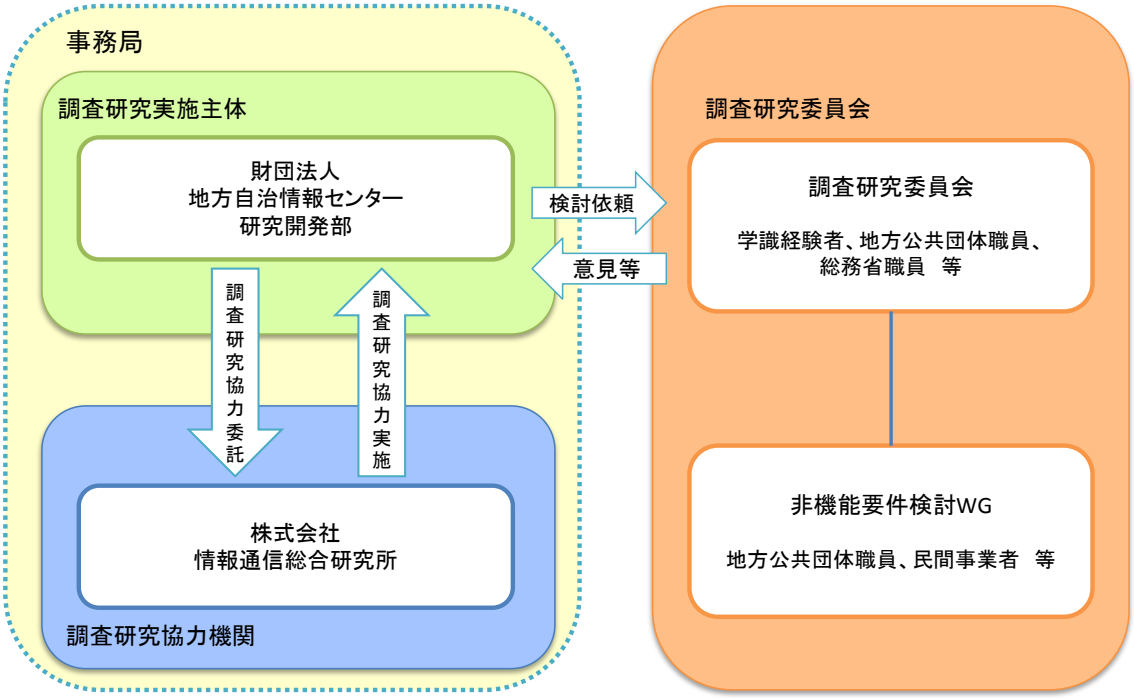


図－4　調査研究のフロー

第３節 実施体制

１　実施体制

本調査研究は、図－5 に示す実施体制で実施する。



図－5　実施体制

２　調査研究委員会及び WG

本調査研究の実施に当たっては、本件に係る専門知識、知見を有する学識経験者、有識者、地方公共団体における情報システム担当職員、民間事業者等で構成する次の調査研究委員会及び WG を設置し、本調査研究の方向性、的確性、適時性、網羅性、地方公共団体のニーズとの合致性等のアドバイスを頂くとともに、幅広い意見、助言等を伺い報告書を作成した。

地方公共団体の情報システム調達仕様書における非機能要件の標準化
に関する調査研究委員会の構成（敬称略　五十音順）

≪委員≫

上杉　卓志	鳥取県	地域振興部情報政策課　参事（IT 統括担当）
鵜飼　陽介	総務省	地域力創造グループ地域情報政策室 電子自治体推進係長
大高　利夫	藤沢市	総務部参事兼 IT 推進課長
大山　水帆	川口市	企画財政部情報政策課長
小林　隆	東海大学	政治経済学部政治学科　専任教授
須貝　俊司	財団法人	地方自治情報センター　理事
山口　秀二	さいたま市	CIO 補佐監

山下　博之　　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センター
システムグループ　グループリーダー

≪非機能要件検討 WG≫

安藤　弘和　　藤沢市　総務部 IT 推進課　主査
上杉　卓志　　鳥取県　地域振興部情報政策課　参事（IT 統括担当）
柄澤　治　　さいたま市　政策企画部 IT 政策課　係長
小林　悠一　　川口市　企画財政部情報政策課　主任
橋本　正義　　さいたま市　政策企画部 IT 政策課　係長
藤間　桂二郎　藤沢市　総務部 IT 推進課　課長補佐

≪オブザーバー≫

株式会社日立製作所
日本電気株式会社
富士通株式会社

≪事務局≫

財団法人地方自治情報センター　研究開発部
株式会社情報通信総合研究所（研究協力機関）

第２章 地方公共団体の情報システム調達仕様書における非機能要件の現状と課題

第１節 非機能要件に関する現状

まず、地方公共団体の非機能要件に関する取組の実態について、地方公共団体等を対象としたヒアリング調査、オブザーバーの意見等を中心に得られた知見を整理する。

１　調査の概要

（１） 調査に協力いただいた地方公共団体・ベンダー

ヒアリング調査に協力いただいた地方公共団体等は以下のとおりである。

・京都府　政策企画部
・鳥取県　地域振興部情報政策課（WG 参加団体）
・さいたま市　政策企画部 IT 政策課（WG 参加団体）
・川口市　企画財政部情報政策課（WG 参加団体）
・豊島区　政策経営部情報管理課
・藤沢市　総務部 IT 推進課（WG 参加団体）
・株式会社日立製作所（WG オブザーバー）
・日本電気株式会社（WG オブザーバー）
・富士通株式会社（WG オブザーバー）

（２） 調査項目

ア 情報システム調達仕様書における非機能要件の定義や標準化に関する現状について

（ア） 情報システム調達仕様書における非機能要件の定義や記載について
（イ） 非機能要件の標準化の取組について
（ウ） 情報システムのレベル分けについて
（エ） 情報システム調達仕様書の作成時におけるチェック体制について
（オ） 情報システム調達仕様書の非機能要件の記載や標準化における問題点について

イ IPA 作成の非機能要求グレードに対する意見

ウ 非機能要求グレード（地方公共団体版）の活用促進のポイント

（３） 調査期間

平成 25 年 7 月～9 月

２　地方公共団体における情報システム調達仕様書の実態

（１） 非機能要件の必要性について

非機能要件という言葉になじみは薄いものの、情報システム部門（以下「ICT 部

門」という。）に対して具体例を示した上で質問すれば、その重要性及び必要性の認識度は高い。非機能要件については、各団体で情報システム調達仕様書のサンプル等を作成し、これを参考に記載しているが、網羅性や適切な要件定義については問題があると感じている。

（２） 非機能要件に関する認識

ほとんどの地方公共団体において、庁内では「非機能要件」という言葉や概念は認知されていないという実態にある。特に、ICT 部門以外の職員は、非機能要件の概念自体をほとんど認識していないという団体が多数であった。

（３） 非機能要件に関する情報システム調達仕様書における記載状況

先述のような認識の中で、一般的に、地方公共団体の情報システム調達仕様書においては、非機能要件として位置づけて、体系的に要件を記載している例は限られる。この点について、地方公共団体の人口等、規模の大小によって異なる傾向がある。都道府県や政令市等、大規模な団体では、機能要件と非機能要件がそれぞれ情報システム調達仕様書に明記されている場合もある。しかし、中小規模の団体では、非機能要件が記載されていないケースが多い。また、中小規模の団体では、非機能要件に当たる項目が、機能要件として記載されている場合がある。また、非機能要件項目の情報システム調達仕様書への記載のレベルについても様々であり、統一されていない。

このような実態からうかがえるように、機能要件という言葉や概念は、地方公共団体職員においても一般化し、情報システム調達仕様書で記載されているが、非機能要件については、一部の大規模な地方公共団体を除いては認知が進んでおらず、情報システム調達仕様書に必要な事項が示されていないケースが多いものと想定される。

３　地方公共団体における非機能要件の定義方法

（１） 情報システム調達仕様書の作成の体制

地方公共団体において情報システムを調達する際、多くの団体において、業務主管部門が主体となって情報システム調達仕様書を作成し、関与の違いはあるが ICT 部門がその作成支援を実施しているという形が多い。支援の内容としては、情報システム調達仕様書のサンプル等の情報提供を行う、あるいは業務主管部門が作成した情報システム調達仕様書を ICT 部門において確認・指導するものである。

情報システム調達仕様書の確認方法は団体ごとに差異があり、標準的な調達ガイドラインを作成し、要件についての抜け漏れ等の確認を実施している団体や、全庁的な会議体により、システム導入の可否決定を行うような体制が組まれている団体もある。

しかし、小規模団体においては、このような確認や支援の体制を組むことが難しいことも多いと想定される。

（２） 地方公共団体の情報システム調達仕様書における非機能要件の標準化

地方公共団体の中には、調達ガイドラインを策定している、あるいは情報システム調達仕様書のサンプルを作成し、業務主管部門に提供している団体もある。このような団体においては、非機能要件項目の一定の標準化が果たされ、設定すべき項目の抜け漏れも防ぐことができる。

しかし、ICT 部門への相談等も不十分であると、情報システムを利用する業務主管部門で非機能要件に該当する項目の数値や妥当性を判断することができず、ガイドラインにおいて規定されているものやサンプル仕様書のまま、一律の数値で情報システム調達仕様書を作成する場合も多いと考えられる。結果、調達対象となる情報システムにおいて適切ではない水準の要件が設定されるおそれがある。特に業務主管部門の視点からはオーバースペックになりがちであり、コストの増加につながる懸念があるとの指摘があった。

（３） 情報システム調達仕様書の作成手順

地方公共団体により違いはあるものの、一般的には、地方公共団体における情報システム調達仕様書は、以下のような流れで作成されているものと想定する。

- 業務主管部門が中心となって、調達内容を検討する。
- 検討に当たっては、過去の情報システム調達仕様書等を基に変更を行うことが多い。
- その際、ICT 部門が情報システム調達仕様書のサンプルの提供やアドバイスを行う。
- 必要に応じて、ベンダーへのヒアリングや RFI（詳細は「利用ガイド」（第２章第７節　１　RFI 等の実施）を参照。）により内容を精査する。
- 検討結果を情報システム調達仕様書として取りまとめる。

検討や確認のレベルは、担当した職員のスキルによるところがあり、作成される情報システム調達仕様書も記載項目や精度がまちまちなものとなっている。業務主管部門だけで、ICT 部門やベンダーへの確認も不十分なまま、情報システム調達仕様書が作成されることも多いと想定される。

（４） 情報システムのレベル分け

情報システムの要件を検討する際には、その重要度等に応じて合理的に要件の定義を行うことが望まれる。このため、重要度等に応じた情報システムのレベル分けを行うことが有益と考えられる。地方公共団体において、情報システムの社会的重要性等を勘案し、適合した非機能要件を定義できている情報システム調達仕様書は少なく、そのような状況の中で非機能要件の標準化を図った場合、過剰な非機能要件により情報システムのコストの増加につながるおそれもある。

実態として、情報システムの明確なレベル分けを実施している地方公共団体は少数であり、レベル分けを実施している地方公共団体においても非機能要件を考慮したレベル分けを実施している地方公共団体はさらに少数であると想定される。

４　地方公共団体の特性

（１） 情報システムの特性

地方公共団体の情報システムについては、都道府県や市区町村で同様な業務を実施していることから、情報システムに求められる要件については、一定の共通性がある。したがって、非機能要件についても比較的標準化を図りやすいものと考えられる。

また、個々の地方公共団体が導入する情報システムは民間企業の情報システムとは性格が異なる面がある。例えば、航空や金融業界の情報システムのような１秒でも止まることが許容されない情報システムとは性格に違いがある。

（２） 調達の特性

地方公共団体における調達は、民間企業に比べて、調達行為も契約行為もより厳密性が求められ、検収についても説明責任が生じる。非機能要件については、例えば稼働率やレスポンスタイム等のような検収が難しい項目がある。

このような項目については、概ね達成できればとよいという「目標値」として示し、運用する過程において検証している、という事例があった。

また、同様に SLM[1]（Service Level Management）の考え方をとる事例もあった。クラウドの導入が進むことに伴い、SLA[2]（Service Level Agreement）が定められる例が増えてきており、SLA の中に非機能要件が定められるケースがある。特に、電子申請等のフロントオフィス系の情報システムでは多くの事例で SLA が整備されている。しかし、それ以外の情報システムにおいては、現時点では SLA の適用例は限られている。また、調査対象団体からは、フロントオフィス系の情報システムも含め、測定や評価等、その運用についての難しさが指摘されている。

---

[1] SLM:service level management の略称。ネットワーク上のサービス品質の測定方式，またはその機能を運用管理に用いる管理ツール。

[2] SLA:service level agreement の略称。ICT 等のサービスのベンダーが、利用者にサービスの品質を保証する制度。

第２節 非機能要件に関する課題

調査結果を踏まえ、地方公共団体における情報システム調達仕様書の非機能要件に関する課題を示す。

１　非機能要件という概念の浸透

地方公共団体の情報システム調達において非機能要件に関する認識は希薄である団体が多数である。非機能要件に対して認識している地方公共団体においても ICT 部門に限ったものであり、業務主管部門では認識されていない。業務主管部門では、業務を実現することに関心が集中してしまい、非機能要件について意識がいかないおそれがある。まずは、非機能要件という概念の浸透が重要な課題である。

２　適切な非機能要件の定義ができる手法の確立

地方公共団体を取り巻く ICT 環境は急速に発展し、また複雑化している。このような環境の中で、地方公共団体の職員、とりわけ業務主管部門による非機能要件の明確化は容易ではない。非機能要件が不明確なまま調達され必要な品質が確保されない、あるいは過剰な要件での調達が実施され情報システムのコストの増加につながることも多く考えられる。ICT 部門とも連携し、業務主管部門主導であっても適正な非機能要件を定義できるような手法を確立することが求められる。

３　発注者と受注者の合意と非機能要件の標準化

コストと品質のバランスのとれた非機能要件が明確に示されないまま情報システムを調達すると、発注者である地方公共団体とシステム構築を受注するベンダーとの間で、要件に関する齟齬が発生し、トラブルが発生するおそれがある。

調達段階において、地方公共団体とベンダーが共通認識をもち、合意形成を図ることが重要であり、非機能要件の標準化の取組が重要であると考える。

４　地方公共団体の特性を考慮した非機能要件の標準化

地方公共団体の情報システムは民間企業の情報システムとは異なる特性がある。非機能要件の標準化の取組については、特に地方公共団体の情報システムを対象としたものは見受けられない。地方公共団体の特性を考慮した非機能要件の標準化の取組が求められる。

また、調達・契約行為についても、民間企業に比べて厳密性が求められる。情報システム調達仕様書における非機能要件の検討においては、このような地方公共団体の組織的な性格についても留意する必要がある。

５　情報システムの調達における職員負担の軽減

大きく変化する社会環境の中で、地方公共団体の業務遂行に情報システムを含む ICT は必要不可欠な手段となっている。ICT の重要性が増す一方で、地方公共団体が求める情報システムを、適切な要求水準を確保しながら適正な金額で調達することは容易ではなく、情報システム調達仕様書の作成は大きな業務負荷ともなっている。

特に小さな団体ほどその負担は重いものと考えられる。

情報システム調達仕様書における記載事項の中でも、検討することの難しい非機能要件の検討については標準的な指標を策定し、検討を簡素化することが求められる。

第３章 非機能要件の標準化の動向

第１節 非機能要求グレードの取組の概要

１　非機能要求グレードとは

非機能要求グレードは、2010 年 4 月に IPA により公開された。情報システムのシステム基盤の可用性や拡張性等の非機能要求を明確化し、システム構築におけるベンダーとユーザ企業間の合意形成を支援する手法である。

非機能要求グレードは表－1 に示す成果物から構成される。

表－1　非機能要求グレードを構成する成果物

No	成果物	内容
1	利用ガイド（解説編）	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したもの。
2	利用ガイド（利用編）	非機能要求グレードの具体的な利用方法について解説したもの。
3	グレード表	3つのモデルシステムと重要な非機能要求項目に対する要求レベルとグレードを一覧表化したもの。グレード表で対象となる要求項目は、発注者の視点を踏まえ、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。
4	項目一覧	システム基盤に関わる非機能要求項目を発注者／受注者間で漏れなく共通に認識できるよう体系化した一覧表。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作成されている。
5	樹系図	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。樹系図はグレード表及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できる。
6	活用シート	グレード表と項目一覧の内容をまとめた一覧表。スプレッドシート形式で、使用条件の範囲で変更が可能としている。

２　非機能要求グレードの特徴

（１） 分類体系

「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」の大項目 6、中項目 34、小項目 116、メトリクス 236 からなる。メトリクスとは小項目を定量的に表現するための指標であり、非機能要求を合意する単位となる。メトリクスのうち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を重要項目と定義し、92 の重要項目がある。

（２） 要求項目のレベル分け

メトリクスに対して、レベルが設定されており、通常取りうる値をレベル 0 から

レベル 5 までの 6 段階で整理したものである。レベルの差は、技術・製品の違いであり、レベル値が大きいほど実現難易度が高く、コストの増加につながる傾向にある。レベルで示す値は、発注者／受注者間で合意形成を図るためのものである。表－2 に要求項目のレベル分けの例を示す。

表－2　要求項目のレベル分けの例

大項目	中項目	小項目	重要項目	メトリクス（指標）	レベル					
					0	1	2	3	4	5
可用性	継続性	業務継続性	○	対象業務範囲	内部向けバッチ系業務	内部向けオンライン系業務	内部向け全業務	外部向けバッチ系業務	外部向けオンライン系業務	すべての業務
			○	サービス切替時間	24 時間以上	24 時間未満	2 時間未満	60 分未満	10 分未満	60 秒未満
			○	業務継続の要求度	障害時の業務停止を許容する	単一障害時は業務停止を許容せず、処理を継続させる	二重障害時でもサービス切替時間の規定内で継続する			

（3）　要求項目のレベル設定

情報システムを表－3 に示す 3 つのモデルシステム（「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」）に分類し、それぞれ非機能要求を具体的に推奨値として定義している。

表－3　要求項目のレベル設定の例

大項目	中項目	小項目	メトリクス（指標）	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
可用性	継続性	業務継続性	対象業務範囲	2	内部向け全業務	内部向けの業務が主要業務であり、内部向け全業務が稼働していることがシステム稼働の条件となる。	3	外部向けバッチ系業務	外部とのバッチ的な処理で業務が主要業務であり、内部向けの業務および外部とのバッチ的な業務が稼働していることがシステム稼働の条件となる。	4	外部向けオンライン系業務	外部とのリアルタイムでの処理が主要業務であり、外部向けオンライン業務が稼働していることがシステム稼働の条件となる。
			サービス切替時間	1	24時間未満	外部向けの業務はなく、1日程度の中断であれば許容できる。 [−] 障害時の対策を必要としない場合 [+] サービス切替の影響がある場合（影響度に応じて中断を許容できる時間を検討する）	3	60分未満	外部とのオンラインでの業務はあるが、数十分の停止までは許容可能。 [+] オンライン業務においてサービス切替の影響がある場合（影響度に応じて中断を許容できる時間を検討する）	5	60秒未満	リアルタイム性が要求されるため、システム停止時は瞬時の復旧が必要となる。 [−] 業務の停止が1時間以内であれば許容できる場合
			業務継続の要求度	1	単一障害時は業務停止を許容せず、処理を継続させる	障害時の業務停止の許容時間に合わせる。 [−] リスクを認識した上、障害発生時の業務停止を許容できる場合 [+] コスト増を考慮した上で二重障害による業務停止を防止する必要がある場合	2	二重障害時でもサービス切替時間の規定内で継続する	障害時の業務停止の許容時間に合わせる。 [−] リスクを認識した上、二重障害での業務停止を許容できる場合	2	二重障害時でもサービス切替時間の規定内で継続する	二重障害でも業務継続が前提となる。

（4） 段階的な要求項目の詳細化

非機能要求グレードは、以下のように要求・合意事項を段階的に詳細化することを前提としている。

ア モデルシステムの選定

グレード表を利用し、実現したい情報システムのイメージ（大まかな非機能要求の状態）から、最も近いモデルシステムを選択する。

イ 重要項目のレベル決定

樹系図を利用しながら、選定したモデルシステムに示されるレベル値（ベース値）を参考に、重要項目のレベルを決定する。

ウ 重要項目以外のレベル決定

開発開始までに必要な要求項目及びそのレベルを決定する。

3 非機能要求グレードの利用効果

（1） 非機能要求グレードのメリット

非機能要求グレードのメリットとしては以下の 3 点が挙げられる。

- 非機能要求を「早期に」判断できる
- 非機能要求を「誤解なく」提示・確認できる
- 非機能要求を「漏らさずに」確認できる

ア 非機能要求を「早期に」判断できる

以下により、非機能要求を「早期に」判断できる。

- 最初は「モデルシステム」でイメージレベルから確認することができる。
- 「グレード表」で重要な項目に絞ってから検討することができる。
- 1 から決めるのではなく、推奨された要求値から「調整」することができる。

イ 非機能要求を「誤解なく」提示・確認できる

以下により、非機能要求を「誤解なく」提示・確認できる。

- 要求レベルで「具体的な選択肢」を提示することができる。
- 「十分に」「しっかりと」のようなあいまいな表現ではなく、「レベル 3 で」と具体的に確認することができる。

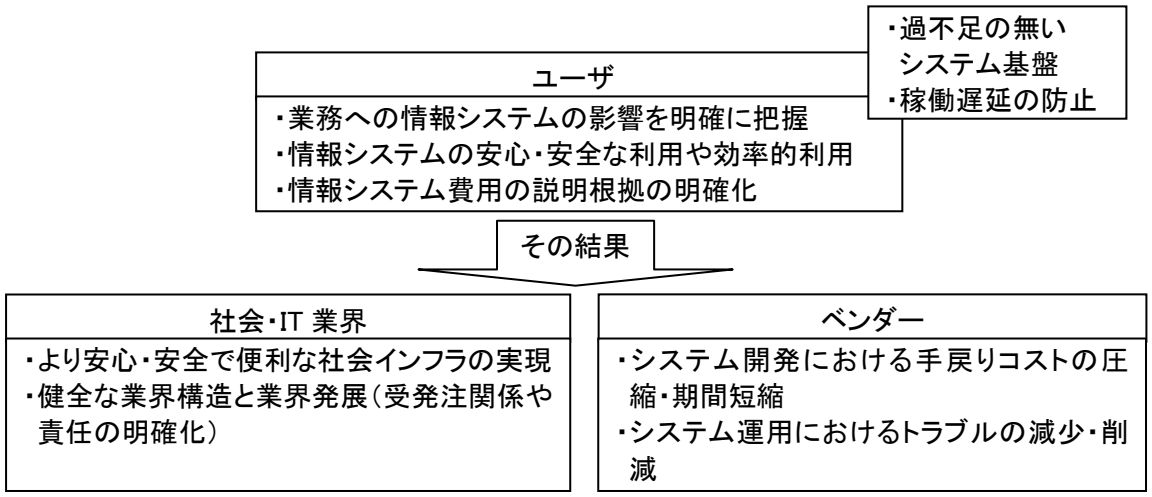
ウ 非機能要求を「漏らさずに」確認できる

以下により、非機能要求を「漏らさずに」確認できる。

- 網羅的な要求項目の一覧をチェックリストとして活用することができる。
- 樹系図による全体を俯瞰することで「矛盾」がないかチェックすることができる。

（２） 「非機能要求グレード」による効果

図－6 に示すように「非機能要求の見える化」を通じ、ユーザ・社会・ベンダーの発展に貢献できる。



出所：IPA 資料を基に作成。

図－6 「非機能要求グレード」による効果

以上、IPA の非機能要求グレードは、非機能要件を検討するに当たって、非常に有効なツールである。地方公共団体の情報システム調達仕様書における非機能要件を検討する際にも、極めて有効であると考えられる。

第 4 章において、IPA の非機能要求グレードを基にした、非機能要求グレード（地方公共団体版）についての考え方を示す。

第４章 非機能要求グレード（地方公共団体版）について

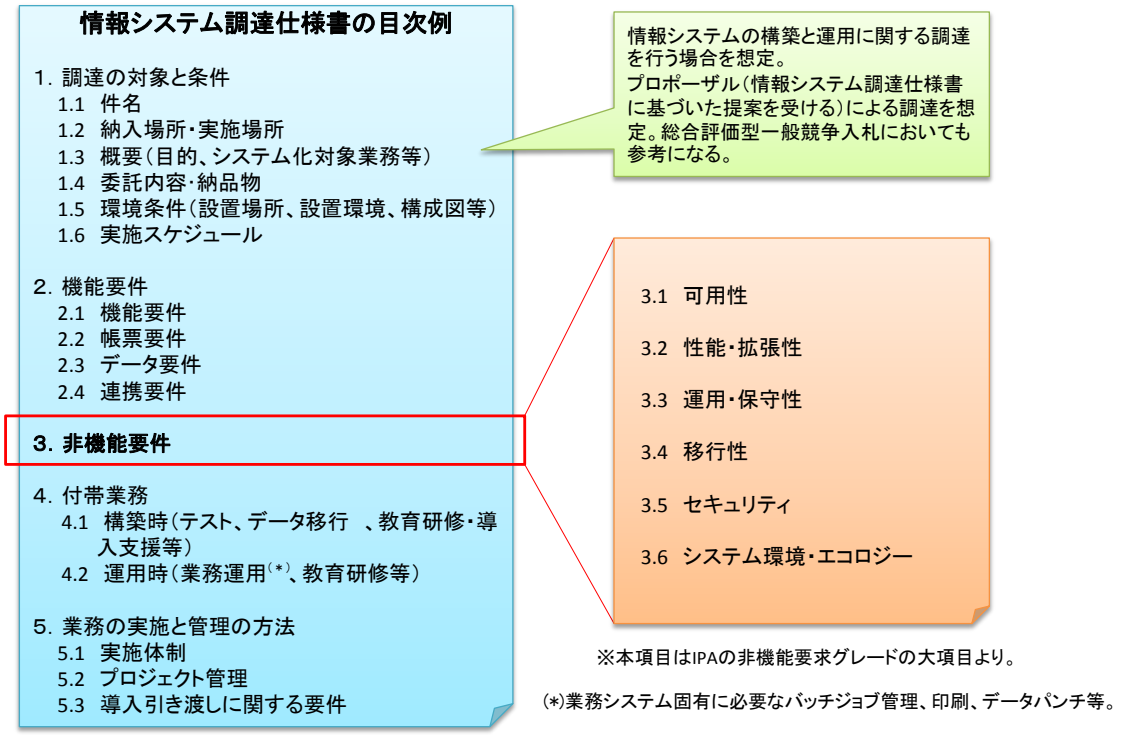
ここでは、地方公共団体の実状等を踏まえ検討・作成した、非機能要求グレード（地方公共団体版）について、その考え方等を説明する。

第１節 基本的な考え方

１　本調査研究の対象範囲

本調査研究は、情報システム調達仕様書に記載される内容のうち、非機能要件を対象範囲としている。情報システム調達仕様書の目次例を図－7 に示す。

非機能要求グレード活用シート（地方公共団体版）は、情報システム調達仕様書の非機能要件部分を作成するためのツールとして位置づける。



図－7　非機能要求グレード（地方公共団体版）の情報システム調達仕様書の中での取扱範囲

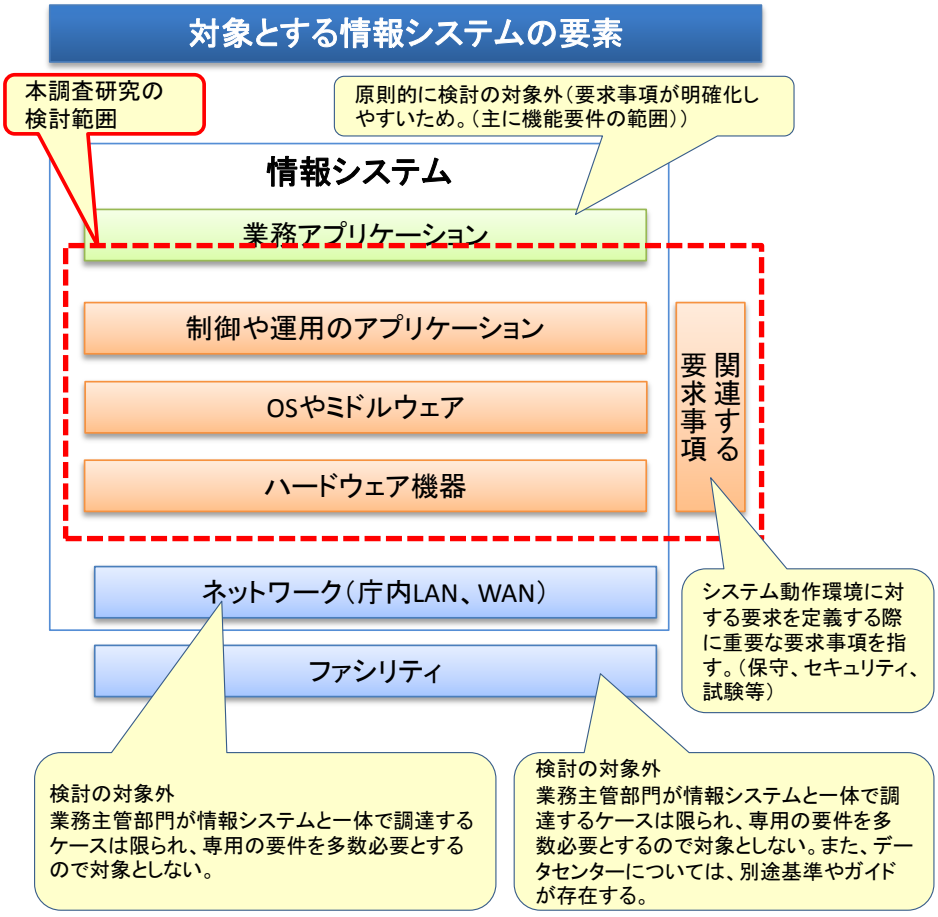
２　対象とする非機能要件の範囲

IPA の非機能要求グレードで対象としている範囲をベースに、情報システム調達仕様書に記載される内容のうち、図－8 に示すシステム動作環境に関わる非機能要件を対象範囲とする。また、業務アプリケーションを定めるための項目も原則的に範囲外とする。

業務アプリケーションについては、主に機能要件の範囲であり、要求事項が明確化しやすいため対象としない。

ネットワークについては、業務主管部門が情報システムと一体で調達するケースは限られ、専用の要件を多数必要とするので対象としない。ただし、セキュリティの観点からのネットワークに関係する項目は対象とする。また、他の情報システムとの連携に関して非機能要件として留意すべき点はないか検討が必要である。

ファシリティについては、業務主管部門が情報システムと一体で調達するケースは限られ、専用の要件を多数必要とするので対象としない。なお、データセンターやマシン室については、別途基準やガイド[3]が存在する。



出所：IPA「非機能要求グレード利用ガイド（解説編）」,2010 年 4 月,p.2 を基に作成

図－8　対象とする非機能要件の範囲

[3] 例として「情報システム安全対策基準」（平成 7 年通商産業省告示 518 号）< http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf >(最終アクセス 2014 年 2 月 4 日)の「五　設置基準」「七　運用基準」等がある。

対象外としている非機能要求項目を表－4 に示す。

表－4　対象外としている非機能要求項目

項目	除外する理由	例
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、発注者／受注者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、移植性等
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、製品等

出所：IPA「非機能要求グレード利用ガイド（解説編）」

３　地方公共団体版で考慮すべき事項

非機能要求グレード（地方公共団体版）を検討するに当たり、「第２章第２節　非機能要件に関する課題」に示した内容を踏まえて考慮すべき事項として、以下のような点が挙げられる。

（１）　非機能要件という概念の浸透

・「非機能要件」という言葉については、庁内ではほぼ認識されていない。
・情報システム調達仕様書について、機能要件に比べて非機能要件は記載が少ない。
→用語を含め、地方公共団体の業務主管部門職員にとっても分かりやすいことが必要となる。

（２）　適切な非機能要件の定義ができる手法の確立

・業務主管部門が実施することが多い。
・その際、ICT 部門が支援していることが多い。
→このような一般的な情報システム調達仕様書の作成手順を踏まえることが必要となる。

（３）　発注者と受注者の合意と非機能要件の標準化

・ベンダーに対して RFI やヒアリングの実施等、合意形成が重要である。
→ベンダーに確認する手順を組み込むことが必要となる。

（４）　地方公共団体の特性を考慮した非機能要件の標準化

・民間企業等との情報システムの特性の違いがある。
・民間企業等との調達・契約行為の性格の違いがある。
→これらの違いを組み込むことが必要となる。

（５）　情報システムの調達における職員負担の軽減

・特に人的余裕のない中小規模の団体では情報システム調達仕様書の作成は負担となる。
→検討項目を精査し、資料のボリュームも削減する。

４　非機能要求グレード（地方公共団体版）の構成

非機能要求グレード（地方公共団体版）の構成は、表－5 に示すとおりである。

表－ 5　非機能要求グレード（地方公共団体版）の成果物と使い方

成果物	概要と使い方
調査研究報告書（本書）	調査研究内容をまとめたもの。 非機能要求グレード（地方公共団体版）の背景や考え方の理解のために参照する。
利用ガイド	非機能要求グレード（地方公共団体版）の利用方法を示したもの。 非機能要求グレード（地方公共団体版）を利用して情報システム調達仕様書を作成する際に参照する。
項目一覧	非機能要件項目の体系を示したもの。 非機能要件の全体像を理解するときに利用する。 また、各地方公共団体において加工することにより、チェックシートや RFI の回答シート等に利用することができる。
活用シート	非機能要件を検討するためのツール（エクセルシート）。 具体的に情報システム調達仕様書における非機能要件の検討作業のために利用する。

５　IPA の非機能要求グレードとの関係

「非機能要求グレード（地方公共団体版）」は、IPA が作成した「非機能要求グレード」2013 年 4 月版を基に地方公共団体が情報システム調達仕様書を検討する際に活用することを主眼に、地方公共団体の業務やその情報システムの特性に併せて一部変更を行っている。

IPA の非機能要求グレードと非機能要求グレード（地方公共団体版）の成果物との対応関係と主な変更の内容は表－6 に示すとおりである。

表－ 6　IPA の非機能要求グレードと地方公共団体版の成果物との対応

IPA の非機能要求グレード		地方公共団体版
①　利用ガイド（解説編）	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したもの。	本「調査研究報告書」が相当。 ・主に IPA の非機能要求グレードを基にどのような考えで地方公共団体版を作成したかについて示している。
②　利用ガイド（利用編）	非機能要求グレードの具体的な利用方法について解説したもの。	「利用ガイド」が相当。 ・情報システム調達仕様書の作成を目的とした利用方法を示している。
③　グレード表	３つのモデルシステムと重要な非機能要求項目に対する要求レベルとグレードを一覧表化したもの。	「活用シート」に集約。 ・モデルシステムは、４つの業務・情報システムのグループに変更。
④　項目一覧	システム基盤に関わる非機能要求項目を発注者／受注者間で漏れなく共通に認識できるよう体系化した一覧表。	「活用シート」に集約。
⑤　樹系図	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。	「項目一覧」が相当。 ・IPA 版は項目数も多いので、一覧性という面で図にする意味があるが、地方公共団体版では、項目数も階層も少なく、図として提供にしても有効性は低い。 ・一覧形式にて提供することにより、加工して RFI の回答シートにする、チェックリストにする、評価表にする等の、利用方法が想定されるので、有益と考えた。

IPA の非機能要求グレード		地方公共団体版
⑥ 活用シート	グレード表と項目一覧の内容をまとめた一覧表。スプレッドシート形式で、使用条件の範囲で変更が可能。	「活用シート」が相当 ・全 236 項目から、地方公共団体が情報システムを調達するために必要な 76 項目に集約（一部項目追加も実施）。 ・項番（例：A.1.1.1）については、元の番号を引き継いでいるが、追加した項目や概念を変更した項目については新たな番号を付与している。 ・地方公共団体の実状に合わせて、用語表現等を調整している。 ・情報システム調達仕様書の作成を目的に、シート構成や各シートの項目についても追加や順番の変更等をしている。

第２節 活用シートの地方公共団体への適用における考え方

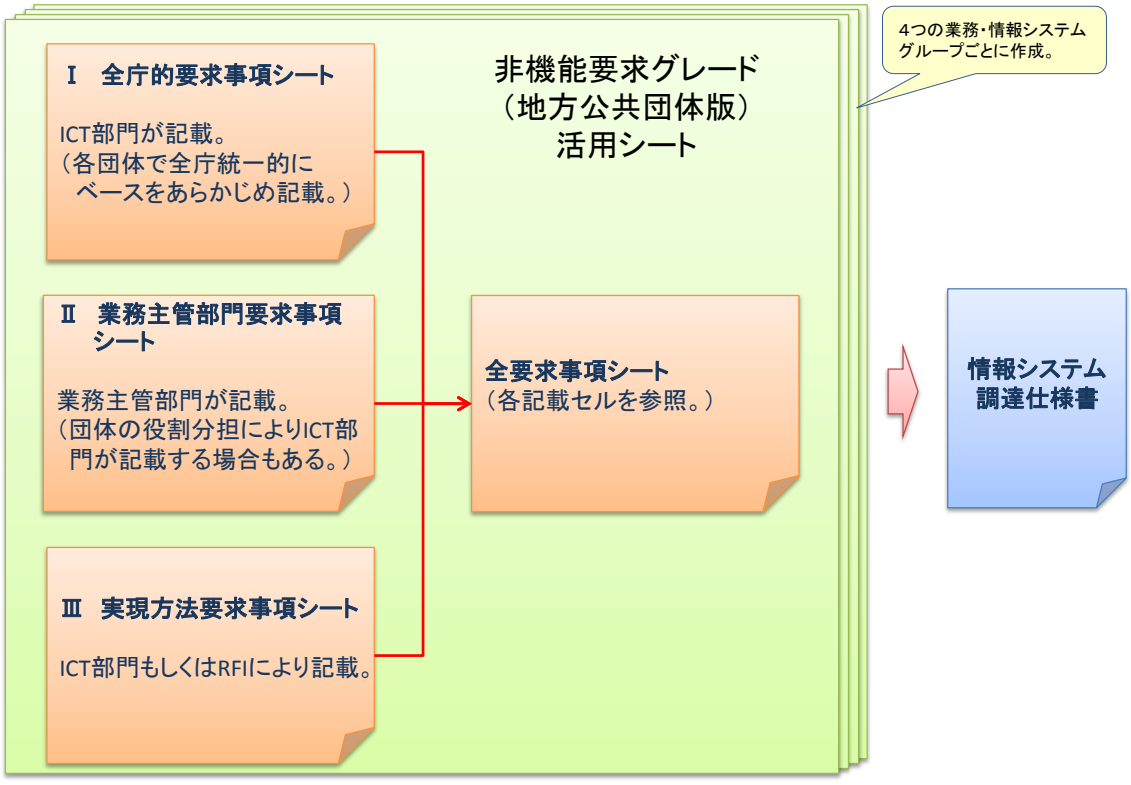
１　活用シートの構成の考え方

非機能要件グレード（地方公共団体版）は、地方公共団体における非機能要件の一般的な手順や役割分担等の実状を踏まえたものとする必要がある。先述のように、地方公共団体では、業務主管部門が中心となって要件定義を行い、ICT 部門がそれを支援するということが多く行われている。また、情報セキュリティを始めとする ICT に関連する規定は、ICT 部門が所管している。

IPA の非機能要求グレードの活用シートでは、ひとつのエクセルファイルに全項目が記載されているが、主な実施者や検討手順に併せて、シートを分けて構成することが、使い勝手の面で有益ではないかと考えた。

また、非機能要件グレード（地方公共団体版）は、情報システム調達仕様書の作成を主眼としているため、検討結果ができる限り情報システム調達仕様書に反映されることが望ましい。

そこで図－9 に示すように、4 つのシートにより構成することとした。

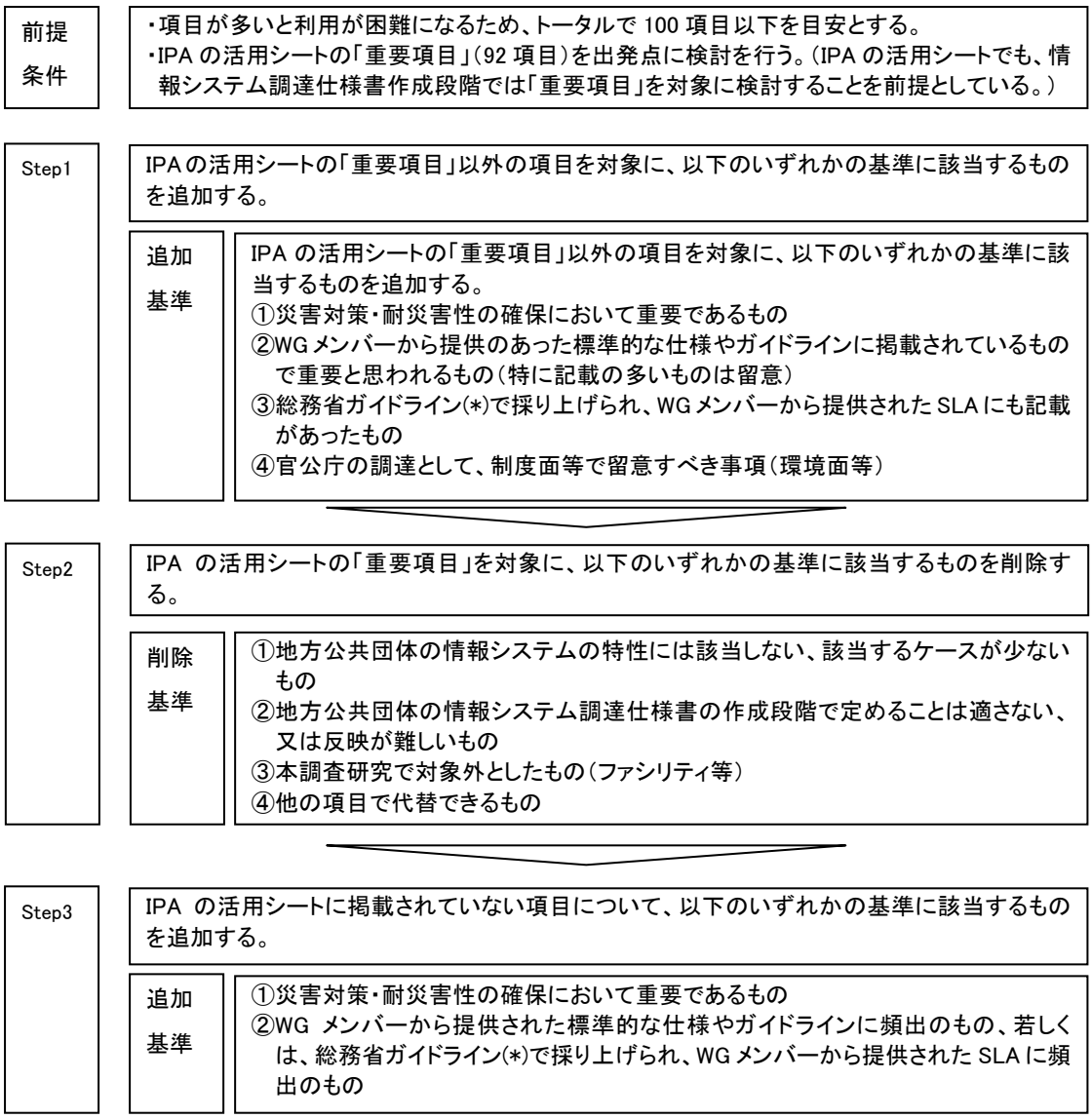


図－9　活用シートの構成

2　活用シートの要件項目（メトリクス）の考え方

（1）　採用項目（メトリクス）の検討

前提条件の下、図－10 に示す手順・基準で非機能要件グレード（地方公共団体版）の活用シートの項目の加除を実施する。



(*)総務省「地方公共団体における ASP・SaaS 導入活用ガイドライン」

図－10　活用シートの項目の加除

（2）　検討結果

IPA の活用シートの重要項目に対して追加・削除を実施し、最終的に全体で 76 項目となった。

ア 重要項目以外の追加項目

IPA の活用シートの中から、重要項目以外の項目で追加したものは表－7 に示す 16 項目である。

表－7　重要項目以外の追加項目

項番	大項目	中項目	小項目	メトリクス(指標)	加除の理由その他備考
A.2.1.1	可用性	耐障害性	サーバ	冗長化（機器）	追加基準①・② サーバの冗長化は耐災害・障害性の観点で重要。
A.2.5.1			ストレージ	冗長化（機器）	追加基準①・② ストレージの冗長化は耐災害・障害性の観点で重要。
A.2.5.3				冗長化（ディスク）	追加基準①・② ディスクの冗長化は耐災害・障害性の観点で重要。
A.3.1.1		災害対策	システム	復旧方針	追加基準① 復旧方針は、災害対策の重要項目
A.3.2.1			外部保管データ	保管場所分散度	追加基準① データの外部保管は、耐災害性の観点で非常に重要。
A.3.2.2				保管方法	追加基準① データの外部保管は、耐災害性の観点で非常に重要。
C.2.3.3	運用・保守性	保守運用	パッチ適用ポリシー	パッチ適用タイミング	追加基準③
C.3.3.1		障害時運用	システム異常検知時の対応	対応可能時間	追加基準②
C.3.3.2				駆けつけ到着時間	追加基準②
C.5.5.1		サポート体制	一次対応役割分担	一次対応役割分担	追加基準② 地方公共団体では、民間に比べ委託することが多いと想定。
C.5.6.2			サポート要員	ベンダー側対応時間帯	追加基準② 地方公共団体では、民間に比べ委託することが多いと想定。
C.5.9.1			定期報告会	定期報告会実施頻度	追加基準③・②
C.5.9.2				報告内容のレベル	追加基準② また、C.5.9.1 とセットとなる内容のため。
D.5.1.1		移行計画	移行作業分担	移行のユーザ/ベンダー作業分担	追加基準②
E.4.3.3	セキュリティ	セキュリティリスク管理	セキュリティパッチ適用	セキュリティパッチ適用タイミング	追記基準③

項番	大項目	中項目	小項目	メトリクス(指標)	加除の理由その他備考
F.5.1.1	システム　環境・エコロジー	環境マネージメント	環境負荷を抑える工夫	グリーン購入法対応度	追加基準④ 環境対策は政府を始め、地方公共団体の調達では重要であり、最低限本項目は必要と考えた。

イ 削除項目

IPA の活用シートの重要項目から削除したものは表－8 に示す 33 項目である。

表－8　重要項目からの削除項目

項番	大項目	中項目	小項目	重複項目	メトリクス(指標)	加除の理由その他備考
A.1.1.1	可用性	継続性	運用スケジュール	○	運用時間（通常）	削除基準④ C.1.1.1 と重複する項目であるため。
A.1.1.2				○	運用時間（特定日）	削除基準④ C.1.1.2 と重複する項目であるため。
A.1.1.3				○	計画停止の有無	削除基準① 本要件は 24 時間稼働が前提の場合に重視される要件。24 時間稼働の情報システムは限られる。
A1.2.1			業務継続性		対象業務範囲	削除基準④ 機能要件を明らかにすれば自ずと示される要件であり、意識的に記載する必要性は少ない。 RLO の点は、別に項目がある
A.1.2.2					サービス切替時間	削除基準④ RTO でほぼ代替できる。
A.1.2.3					業務継続の要求度	削除基準② 障害の内容や導入されるシステム構成等も考慮し設計しないと仕様として示せない。
A.4.2.1		回復性	可用性確認		確認範囲	削除基準② テスト項目のひとつと考えられ、本項目を取り立てて情報システム調達仕様書に記載する意義は少ないと考える。
B.3.1.1	性能・拡張性	リソース拡張性	CPU 拡張性		CPU 利用率	削除基準② 調達時には決定しにくいため。
B.3.1.2					CPU 搭載余裕有無	削除基準② 空きスロットまで示すことは難しいと考える。 仮想環境下ではハード資源の融通がしやすくなっている。

項番	大項目	中項目	小項目	重複項目	メトリクス(指標)	加除の理由その他備考
B.3.2.1			メモリ拡張性		メモリ利用率	削除基準② 調達時には決定しにくいため。
B.3.2.2					メモリ搭載余裕有無	削除基準② 空きスロットまで示すことは難しいと考える。 仮想環境下ではハード資源の融通がしやすくなっている。
C.1.2.6	運用・保守性	通常運用	バックアップ		バックアップ保存期間	削除基準④ 「B1.3.1 保管期間」「C1.2.5 全体バックアップの取得間隔」で代用できる。
C.1.3.2			運用監視		監視間隔	削除基準② 調達段階で、監視間隔を明確にすることは難しい。
C.2.1.1		保守運用	計画停止	○	計画停止の有無	削除基準① 本要件は 24 時間稼働が前提の場合に重視される要件。24 時間稼働の情報システムは限られる。
C.2.2.1			運用負荷削減		保守作業自動化の範囲	削除基準① 自動化できる作業は、可能な限り自動化することが一般的であるため。
C.6.1.1		その他の運用管理方針	内部統制対応		内部統制対応の実施有無	削除基準① 民間企業向けの IT 統制を意識したものと考えられ、地方公共団体の情報システム調達の対象としては重要ではないと考える。
D.2.1.1	移行性	移行方式	システム展開方式		拠点展開ステップ数	削除基準① 本項目は、全国、全世界等広域に事業所等を持つ組織に適用される項目と考える。
D.2.1.2					業務展開ステップ数	削除基準① 本項目は、全国、全世界等広域に事業所等を持つ組織に適用される項目と考える。
D.4.1.2		移行対象(データ)	移行データ量		移行データ形式	削除基準② 移行データ形式を情報システム調達時に指定することは少ないと考える。
E.3.1.1	セキュリティ	セキュリティ診断	セキュリティ診断		ネットワーク診断実施の有無	削除基準① 地方公共団体の情報システムにおいては、ネットワーク診断は、監査業務等で別途行われることが多く情報システムと同時に調達することは少ないと考える。

項番	大項目	中項目	小項目	重複項目	メトリクス(指標)	加除の理由その他備考
E.7.1.2		不正追跡・監視	不正監視		ログ保管期間	削除基準② 調達段階で、対象を含めて保管期間を明確にすることは難しいと考える。
E.7.1.4					不正監視対象(ネットワーク)	削除基準① 地方公共団体の情報システムにおいては、ネットワーク機能の一部として調達され、情報システムと同時に調達することは少ないと考えられる。
E.7.1.5					不正監視対象(侵入者・不正操作等)	削除基準① 地方公共団体の情報システムにおいては、ネットワーク機能の一部として調達され、情報システムと同時に調達することは少ないと考えられる。
E.8.1.1		ネットワーク対策	ネットワーク制御		通信制御	削除基準① 地方公共団体の情報システムにおいては、ネットワーク機能の一部として調達され、情報システムと同時に調達することは少ないと考えられる。
E.8.2.1			不正検知		不正通信の検知範囲	削除基準① 地方公共団体の情報システムにおいては、ネットワーク機能の一部として調達され、情報システムと同時に調達することは少ないと考えられる。
E.8.3.1			サービス停止攻撃の回避		ネットワークの輻輳対策	削除基準① 地方公共団体の情報システムにおいては、ネットワーク機能の一部として調達され、情報システムと同時に調達することは少ないと考えられる。
E.9.1.1		マルウェア対策	マルウェア対策		マルウェア対策実施範囲	削除基準① 地方公共団体の情報システム全体に関する内容であり、個別の情報システム調達時に、検討すべき内容では無い。
F.2.1.1	システム　環境・エコロジー	システム特性	ユーザ数	○	ユーザ数	削除基準④ B.1.1.1 と重複する項目であるため。
F.2.3.1			拠点数		拠点数	削除基準① 地方公共団体の情報システムにおいては、設置場所を記載する。

項番	大項目	中項目	小項目	重複項目	メトリクス(指標)	加除の理由その他備考
F2.4.1			地域的広がり		地域的広がり	削除基準① 地方公共団体の情報システムにおいては、自ずと設置場所・利用場所は限定されるため。
F.4.1.1		機材設置環境条件	耐震/免震		耐震震度	削除基準③ ファシリティに関する項目であるため。
F.4.2.1			スペース		設置スペース制限(マシンルーム)	削除基準③ ファシリティに関する項目であるため。
F.4.2.2					設置スペース制限(事務所設置)	削除基準③ ファシリティに関する項目であるため。

ウ 新たな追加項目

IPA の活用シートに無く、新たに追加した項目は表－9 に示す 1 項目である。

表－9　新たな追加項目

項番	大項目	中項目	小項目	メトリクス(指標)	備考
C.3.3.4	運用・保守性	障害時対応	システム異常検知時の対応	障害検知通知時間	追加基準②

３　活用シートの掲載項目等

（１） 掲載項目等

地方公共団体での利用を考慮し、以下の点を変更している。

・A4 サイズに収まるように、業務・情報システムごとにシート（エクセルファイル）を分け、見やすいようベース値の設定欄を左側に移動。
・併せて「小項目」「重複項目」「重要項目」「運用コストへの影響」を削除。
・「小項目説明」を削除し、「メトリクス（指標）の説明」を追加。
・「クラウド調達時の扱い」「検収時の扱い」「利用ガイドの解説」欄を追加。
・備考欄の記載内容のうち、地方公共団体職員が必ずしも理解する必要がないと思われる記述の削除。
・レベルに「－（仕様の対象としない)」「＊（ベンダーによる提案事項とする)」を追加。

（２） 概念の変更

一部のメトリクスではメトリクスの解釈やレベル設定の考え方を、地方公共団体の実状に合わせた概念に見直している。なお、このような変更を行った場合には、IPA の非機能要求グレードから項目の概念が変わっていることが分かるように、新しい項番を振っている。

また、レベル値（0～5）の幅が、必ずしも地方公共団体の情報システムに合わないものがあり、変更を加えたメトリクスがある。

表－10 に概念を変更した項目を示す。

表－10　概念を変更した項目

項番	大項目	中項目	小項目	現行の指標（メトリクス）	現行のレベル設定		新項番	指標の見直し結果	レベル設定の見直し結果
B.2.1.1	性能・拡張性	性能目標値	オンラインレスポンス	通常時レスポンス順守率	・順守率を定めない ・60% ・80% ・90% ・95% ・99%以上		B.2.1.4	通常時オンラインレスポンスタイム	・規定しない ・10 秒以内 ・5 秒以内 ・3 秒以内 ・1 秒以内
B.2.1.2				ピーク時のレスポンス順守率			B.2.1.5	アクセス集中時のオンラインレスポンスタイム	

項番	大項目	中項目	小項目	現行の指標（メトリクス）	現行のレベル設定		新項番	指標の見直し結果	レベル設定の見直し結果
C.2.3.3	運用・保守性	保守運用	パッチ適用ポリシー	パッチ適用タイミング	・パッチを適用しない ・障害発生時にパッチ適用を行う ・定期保守時にパッチ適用を行う ・新規のパッチがリリースされるたびに適用を行う		C.2.3.5	OS 等パッチ適用タイミング	・パッチを適用しない ・障害発生時にパッチ適用を行う ・定期保守時にパッチ適用を行う ・緊急性の高いパッチのみ即時に適用を行う。 ・緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う ・新規のパッチがリリースされるたびに適用を行う
C.4.4.2		運用環境	リモートオペレーション	リモート操作の範囲	・リモート操作を行わない ・定型処理のみリモート操作を行う ・任意のリモート操作を行う		C.4.4.3	リモート操作時の接続方法	・リモート操作を行わない ・リモート操作の必要時のみ接続する ・常時接続環境においてリモート操作を行う
C.5.1.1		サポート体制	保守契約（ハードウェア）	保守契約（ハードウェア）の範囲	・保守契約を行わない ・ベンダーの自社製品（ハードウェア・ソフトウェア）に対してのみ保守契約を行う ・マルチベンダのサポート契約を行う（一部対象外を許容） ・マルチベンダのサポート契約を行う（システムを構成する全製品を対象）		C.5.1.2	保守契約（ハードウェア）の種類	・保守契約を行わない ・随時保守（センドバック） ・定額保守（センドバック） ・随時保守（オンサイト） ・定額保守（オンサイト）
C.5.2.1			保守契約（ソフトウェア）	保守契約（ソフトウェア）の範囲			C.5.2.2	保守契約（ソフトウェア）の種類	・保守契約を行わない ・問合せ対応 ・アップデート
E.4.3.3	セキュリティ	セキュリティリスク管理	セキュリティパッチ適用	セキュリティパッチ適用タイミング	・セキュリティパッチを適用しない ・障害パッチ適用時に合わせて実施 ・定期保守時に実施 ・パッチ出荷時に実施		E.4.3.4	ウィルス定義ファイル適用タイミング	・定義ファイルを適用しない ・定期保守時に実施 ・定義ファイルリリース時に実施

（３） 表現の調整等

ICT のスキルが必ずしも高くない地方公共団体職員、特に業務主管部門の職員でも利用できるように、難解と思われる箇所については、文章の平易化を行うとともに用語集の充実を図った。用語集は、利用ガイドの「用語集」として添付している。

また、地方公共団体が良く使用すると考えられるレベルの増減も実施している。

図－11 及び図－12 に、調整の例を示す。

（変更前）

項番	メトリクス	レベル					
		0	1	2	3	4	5
C.4.4.1	リモート監視地点	リモート監視を行わない	構内 LAN を介してリモート監視を行う	遠隔地でリモート監視を行う			

地方公共団体の利用方法に合致した表現に変更

（変更後）

項番	メトリクス	レベル					
		0	1	2	3	4	5
C.4.4.1	リモート監視地点	リモート監視を行わない	庁内 LAN を介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う			

図―11　リモート監視地点における表現の見直し

（変更前）

項番	メトリクス	レベル					
		0	1	2	3	4	5
A.1.5.1	稼働率	95%以下	95%	99%	99.9%	99.99%	99.999%

地方公共団体でよく使用するレベルに変更

（変更後）

項番	メトリクス	レベル					
		0	1	2	3	4	5
A.1.5.1	稼働率	規定しない	95%	99%	99.5%	99.9%	99.99%

図－12　稼働率に関するレベルの見直し

第３節 業務・情報システムの分類の考え方

IPA の非機能要求グレードでは、「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」の 3 つのモデルシステムを用意し、それぞれのベース値を設定している。

地方公共団体の情報システムでは、必ずしもこの 3 つのモデルシステムが適切ではないと考え、非機能要求グレード（地方公共団体版）では、地方公共団体の実状に沿った業務・情報システムの分類を検討した。

１　分類軸の設定

情報システムの安定的なサービスの提供という観点から見たときに、「平常時」にだけ稼働すればよい情報システムと、稼働に必要な資源が喪失する可能性のある「災害時」においても稼働させる必要がある情報システムでは、求める非機能要件のレベルに大きな違いが出ると考えられる。そこで、分類軸として、まず、「平常時」「災害時」の 2 軸で分類することが有益と考える。

（１） 平常時の分類

平常時の分類については、業務及び情報システムが扱う情報資産の観点から分類することが重要と考える。多くの地方公共団体が参照し、これに沿ってマネージメントしていると考えられる、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」[4]の「ひな形」における情報資産分類の考え方に沿うことが有益と考える。

「機密性」「完全性」「可用性」の情報セキュリティの 3 つの観点のうち、安定的な情報システムの運用という観点では「可用性」がポイントとなる。同ガイドラインでは、「可用性」について、「行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産」と定義されている。住民の権利侵害、行政事務の安定的な遂行の観点では、社会に与える影響に違いがあると考えられるため、表－11 の左側のように 3 つに分類することが考えられる。

一方、地方公共団体では、機密性、完全性、可用性の 3 つの観点からの情報資産分類ではなく、4 段階の重要性分類で分類しているケースも多いと考えられる。この重要性分類について、先の可用性に基づく分類に対応させると、おおむね表－11 の右側の区分が対応するものと考えられる。

---

[4] 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」< http://www.soumu.go.jp/main_content/000087555.pdf>(最終アクセス 2014 年 2 月 4 日)

表—11　平常時の分類

項番	「可用性」による分類		重要性分類	
	分類	分類基準	分類	分類基準
1	可用性2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害されるおそれがある情報資産。	Ⅰ	個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
2	可用性2’	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産。	Ⅱ	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
3	可用性1	可用性2の情報資産以外の情報資産。	Ⅲ	外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
			Ⅳ	上記以外の情報。

出所：総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」を基に作成。

（２） 災害時の分類

災害時の業務・情報システムの分類については「地方公共団体における ICT 部門の業務継続計画（BCP)策定に関するガイドライン」「ICT 部門の業務継続計画＜初動版解説書＞」の考え方に沿い、「災害対策として利用するか」「利用しないか」に分類される。

さらに、「災害対策として利用する」情報システムについては、初動対応が必要なもの、不必要なものに分類されるため、合計 3 つに分類される。

災害時の分類については、同様に多くの地方公共団体が参照し、実際にこれに沿ってマネージメントしていると考えられる、「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」[5]「ICT 部門の業務継続計画＜初動版解説書＞」[6]の考え方に沿うことが有益と考える。

具体的には、表－12「業務の影響度の分類」のような分類が考えられる。

5　総務省「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」< http://www.soumu.go.jp/main_content/000145527.pdf>(最終アクセス 2014 年 2 月 4 日)。

6 総務省「ICT 部門の業務継続計画＜初動版解説書＞」<http://www.soumu.go.jp/main_content/000222227.pdf> (最終アクセス 2014 年 2 月 4 日)

表－12　業務の影響度の分類

分類		細目		分類基準
１災害対策として利用する	①　初動対応要	目標開始時間	1 時間以内	応急業務のうち、発災後、直後の対応が求められる業務
			3 時間以内	応急業務のうち、発災後、速やかに対応すべき業務
			6 時間以内	平常時の業務に戻すために初動で必要になる対応業務
	②初動対応不要	影響の重大性Ⅴ　(*)		初動対応は不要だが、影響の重大性がⅤの情報システム
		影響の重大性Ⅳ　(*)		初動対応は不要だが、影響の重大性がⅣの情報システム
		影響の重大性Ⅲ　(*)		初動対応は不要だが、影響の重大性がⅢの情報システム
		影響の重大性Ⅱ　(*)		初動対応は不要だが、影響の重大性がⅡの情報システム
		影響の重大性Ⅰ　(*)		初動対応は不要であり、影響の重大性もⅠの情報システム
２災害対策として利用しない		－		災害対策としては利用が想定されないもの

(*)「表－13　影響の重大性の評価基準」を参照

出所：「地方公共団体におけるに ICT 部門の業務継続計画（BCP）策定に関するガイドライン」「ICT 部門の業務継続計画＜初動版解説書＞」を基に整理

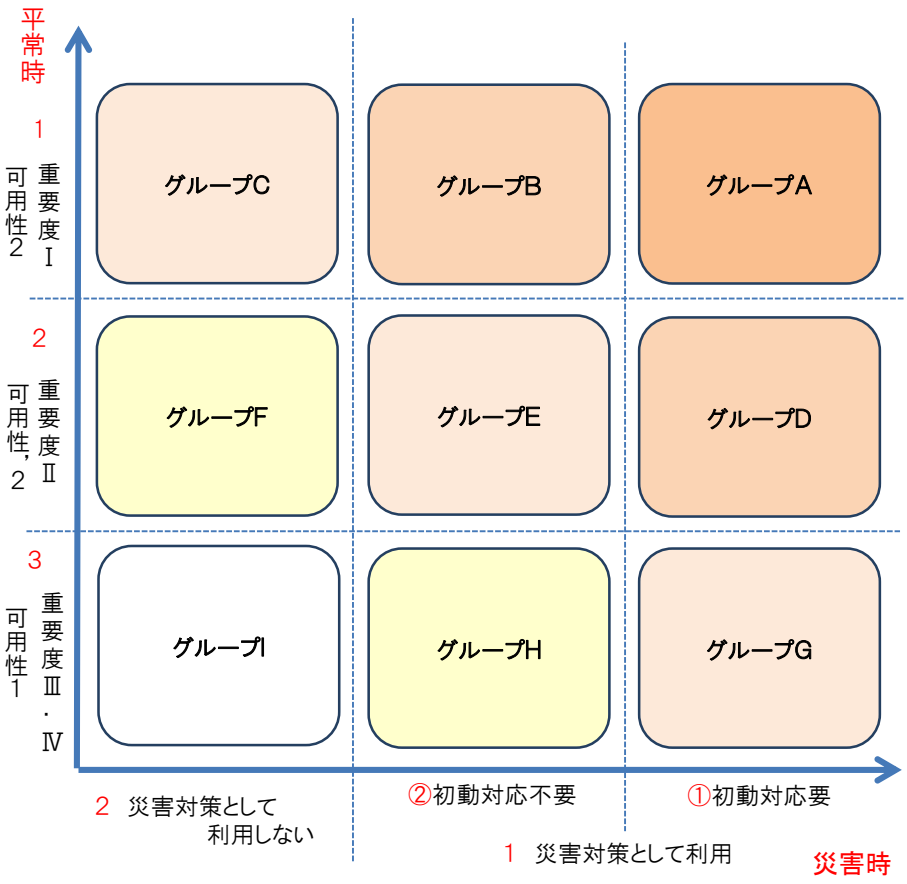
表－13　影響の重大性の評価基準

影響の重大性		対象とする目標レベルに到達していないことに伴う代表的な影響の内容
Ⅴ	甚大	対象とする目標レベルに対象時間までに到達しなかったことにより甚大な社会的影響が発生する。 大規模な社会的批判が発生し、大部分の人はその行政対応は許容可能な範囲外であると理解する。
Ⅳ	大きい	対象とする目標レベルに対象時間までに到達しなかったことにより相当の社会的影響が発生する。 社会的批判が発生し、過半の人はその行政対応は許容可能な範囲外であると理解する。
Ⅲ	中程度	対象とする目標レベルに対象時間までに到達しなかったことにより社会的影響が発生する。 社会的批判が一部で生じ、過半の人はその行政対応は許容可能な範囲であると理解する。
Ⅱ	小さい	対象とする目標レベルに対象時間までに到達しなかったことにより若干の社会的影響が発生する。 しかし、大部分の人はその行政対応は許容可能な範囲であると理解する。
Ⅰ	軽微	対象とする目標レベルに対象時間までに到達しなかったことによる社会的影響はわずかにとどまる。 ほとんどの人は全く意識しないか、意識をしてもその行政対応は許容可能な範囲であると理解する。

出所：内閣府「中央省庁業務継続ガイドライン」

（３）　「平常時」「災害時」によるグループの策定について

整理した「平常時」「災害時」の分類詳細を基に「平常時」を縦軸、「災害時」を横軸に取ることで、図－13 に示す A～I の 9 つの業務・情報システム分類グループを策定した。



図－13　災害時の情報システム分類

２　レベル設定の考え方

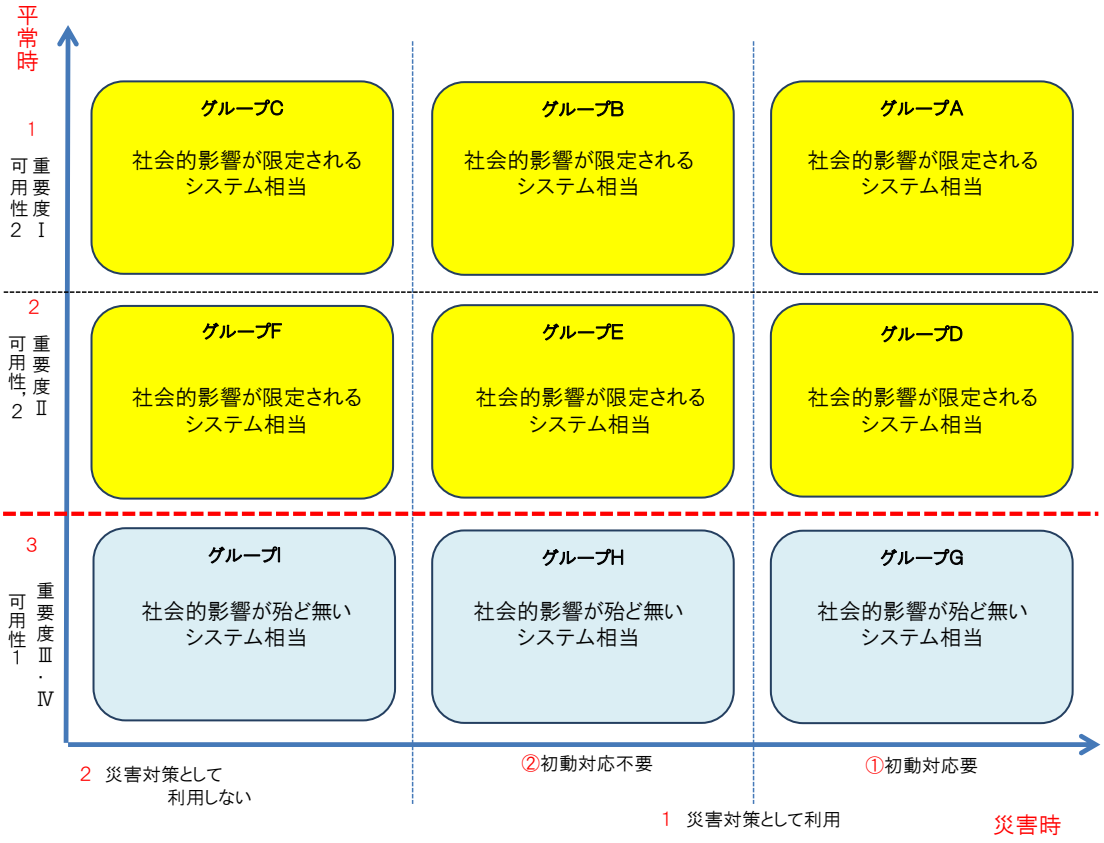
（１）　平常時の対応から見たレベル設定の考え方

業務・情報システムの分類についてのグループを集約する上で、平常時の分類に対し、IPA の非機能要求グレード「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」の 3 つのうちどれが最も近いかを検討した結果を表－14 に示す。

表－14　平常時の対応から見たレベル設定の考え方

縦軸レベル	考え方
平常時1	「社会的影響が限定されるシステム」を割り当てる。（以下、理由） ●「社会的影響が極めて大きいシステム」は、24 時間運用で年間数分程度の停止時間までしか許容できない情報システムであり、地方公共団体の情報システムにはオーバースペックである。 ●「社会的影響が殆ど無いシステム」は、障害時に1日程度の停止時間が許容される情報システムであり、例えば住民記録システムを想定しても、そこまで許容できる情報システムではなく、十分ではない。
平常時2	「社会的影響が限定されるシステム」を割り当てる。（以下、理由） ●「社会的影響が極めて大きいシステム」は、24 時間運用で年間数分程度の停止時間までしか許容できない情報システムであり、地方公共団体の情報システムにはオーバースペックである。 ●「社会的影響が殆ど無いシステム」は、障害時に1日程度の停止時間が許容される情報システムであり、例えば財務会計関連システムを想定しても、そこまで許容できる情報システムではなく、十分ではない。
平常時3	「社会的影響が殆ど無いシステム」を割り当てる。（以下、理由） ●「社会的影響が殆ど無いシステム」は、障害時に1日程度の停止時間が許容される情報システムであり、例えば人口統計システム等は1日程度停止した場合であっても住民及び社会への影響は無い。

この方針に基づいて、IPA の非機能要求グレードのモデルシステムを業務・情報システムの分類に適用すると、図－14 のようになる。



図－14　平常時の対応から見たレベル設定の考え方

（２） 災害時の対応から見たレベル設定の考え方

平常時と同様に業務・情報システムの分類についてのグループを集約する上で、災害時の対応について検討すると、第一に災害時の RTO（目標復旧時間）がポイントとなる。

IPA の「事業継続のための高回復力システム基盤導入ガイド」[7]ではモデルを 4 段階に設定しており、災害時の RTO が短時間になるほど、ハードウェアの信頼性対策やバックアップに関する非機能要件が高度なものとなる。

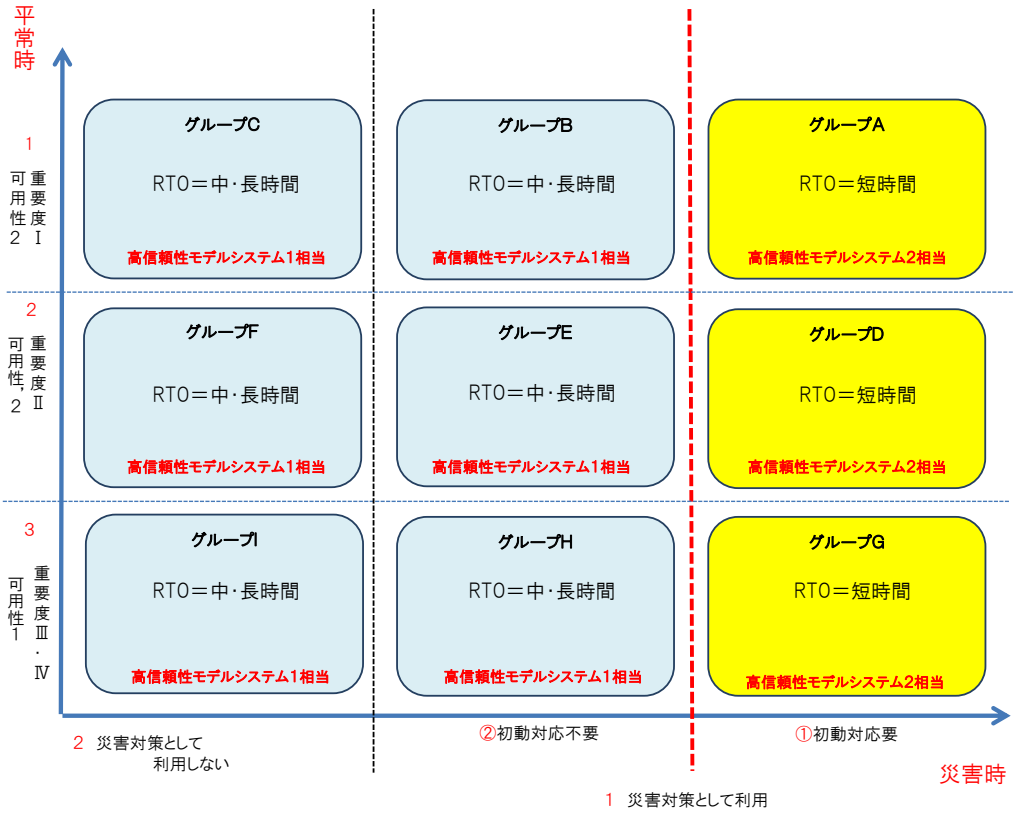
上記の考え方を基に整理した結果を表－15 に示す。

表－15　災害時の対応から見たレベル設定の考え方

横軸レベル	考え方
1－①災害時初動対応要	「災害時の RTO＝短時間」とする。 災害時の RTO を短時間＝3日以内を想定すると、IPA「事業継続のための高回復力システム基盤導入ガイド」における高信頼性モデルシステム3相当以上となる。 高信頼性モデルシステム3は DR（ディザスタ・リカバリ）サイト構築を前提としており、地方公共団体の情報システム実態と比較しレベルが高すぎる。 よって、レベルを下げ高信頼性モデルシステム2相当とした。
1－②災害時初動対応不要 2 災害対策として利用しない	「災害時の RTO＝中・長時間」とする。 災害時の RTO を中時間＝1ケ月、長時間＝数か月と想定すると、共に「事業継続のための高回復力システム基盤導入ガイド」における高信頼性モデルシステム1相当に該当する。 そのため、災害時の RTO＝中時間と RTO＝長時間は同等のレベルとすることが妥当である。

災害時の RTO（目標復旧時間）に対応する対策の観点を、業務・情報システムの分類に適用すると、図－15 のようになる。

[7]独立行政法人　情報処理推進機構「事業継続のための高回復力システム基盤導入ガイド」< http://www.ipa.go.jp/sec/softwareengineering/reports/20120508.html >(最終アクセス 2014 年 2 月 4 日)

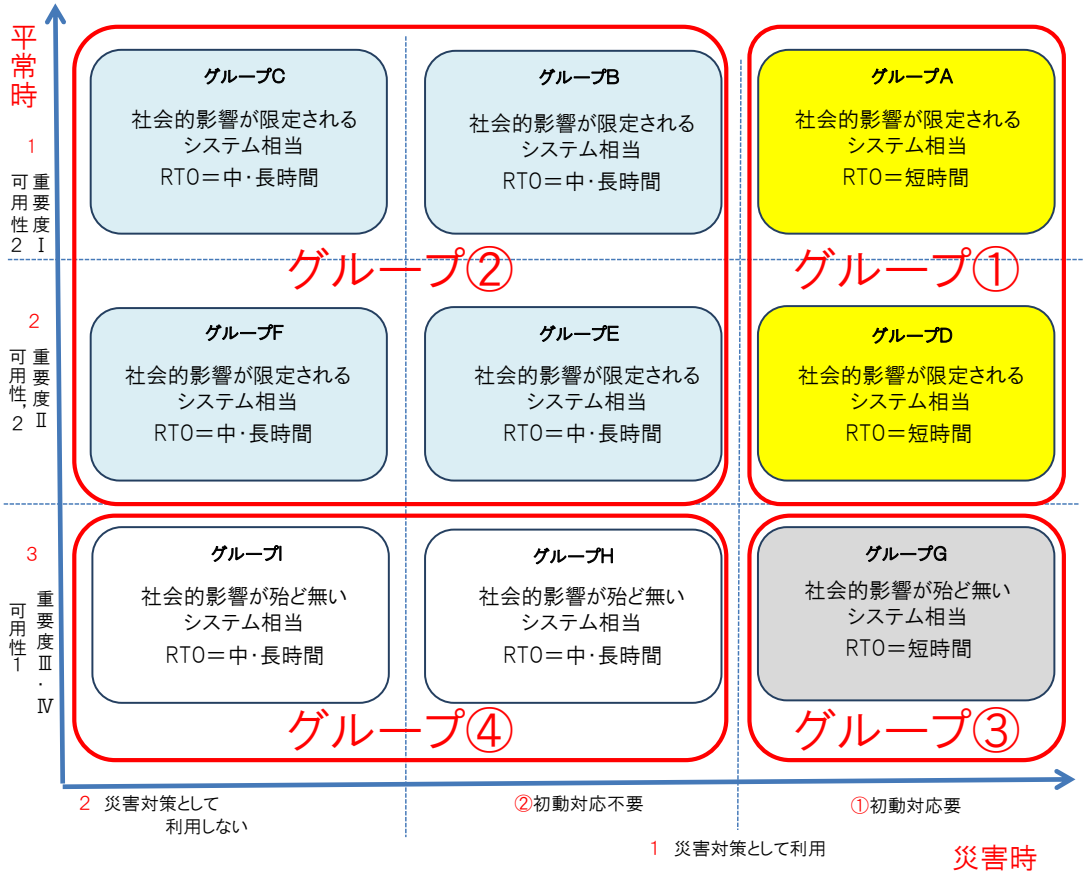


図－15　災害時の対応から見たレベル設定の考え方

（３）　業務・情報システムの分類についてのグループ集約方針について

地方公共団体における非機能要件を検討する上での業務・情報システムの分類グループは、A～I の 9 に分類していたグループを、「平常時」「災害時」の考え方に基づいて、図－16 に示す 4 つに集約することとした。

（例えば、同じグループ②に属するグループ B・C・E・F は概ね同じようなレベルになるが、数項目については差をつける等の調整が発生する可能性がある。）



図－16　業務・情報システムの分類についてのグループ集約方針

（４）　業務・情報システム分類のグループ①～④における情報システム主要要件に関する特徴

集約した、業務・情報システム分類グループからの要求レベルに基づきグループ①～④の主要要件を表－16 のように設定した。

表－16　グループ①～④における情報システム主要要件

		情報システムの分類			
		グループ①	グループ②	グループ③	グループ④
グループ分類からの要求レベル	RTO（主に災害時対策に影響）	短時間	中・長時間	短時間	中・長時間
	データの重要度	高	高	低	低
グループの主要要件（災害対策）	バックアップ間隔	1日1回	1日1回	1日1回	週1回
	サーバ等冗長化（予備機の準備を含む）	あり（予備機の設置場所は遠隔地を推奨）	あり	あり	なし
	遠隔地へのバックアップデータ保管	あり	あり	なし	なし
グループの主要要件（セキュリティ対策）	認証方式	1回（ID／パスワードのみ等）			
	暗号化対策（通信路）	内部ネットワークでは、認証情報（パスワード等）のみ暗号化 外部ネットワークでは、重要情報をSSL等で暗号化			
	暗号化対策（保存データ）	認証情報（パスワード等）のみ暗号化			

（５）　地理的条件の考慮

故障対応をするためのベンダーサポートは、サポート拠点からの距離等といった地理的条件により、大きく異なる。地理的条件は駆けつけ到着時間、稼働率等に大きく影響を与える。全国の地方公共団体は地理的条件に恵まれた団体ばかりでは無いため、表－17 に示すところの全国平均レベルの地理的条件レベルを想定し、レベル設定を行っている。

表－17　レベル設定に当たり候補となる地理的条件レベル

地理的条件レベル	想定する地理的条件	考え方
好条件	県庁所在地及び近隣団体（サポート拠点から車で 1 時間以内の移動距離を想定）	このレベルを標準とすると中小の地方公共団体の実態に比較し、高すぎるレベルとなってしまう。
全国平均レベル	県庁所在地から遠方の団体（サポート拠点から車で 2 時間前後の移動距離を想定）	全国における中小の地方公共団体の最も多くがこのレベルに該当すると推測し、このレベルに設定する。
悪条件	離島等（サポート拠点からフェリー等を利用するため、移動時間が予測できない）	最低条件の見極めが難しい。また、このレベルに合わせることは、他団体にとって現実的で無い。

３　情報システムの分類

情報システムの分類を決定するに当たり、WG メンバー・オブザーバーへのアンケートを実施し、集計結果を基に議論及び調整を実施した。アンケート結果については【参考資料 1】「業務・情報システムアンケートについて」を参照すること。

対象とした都道府県の業務及び情報システム例を表－18 に示す。

表－18　対象とした都道府県の業務及び情報システム例

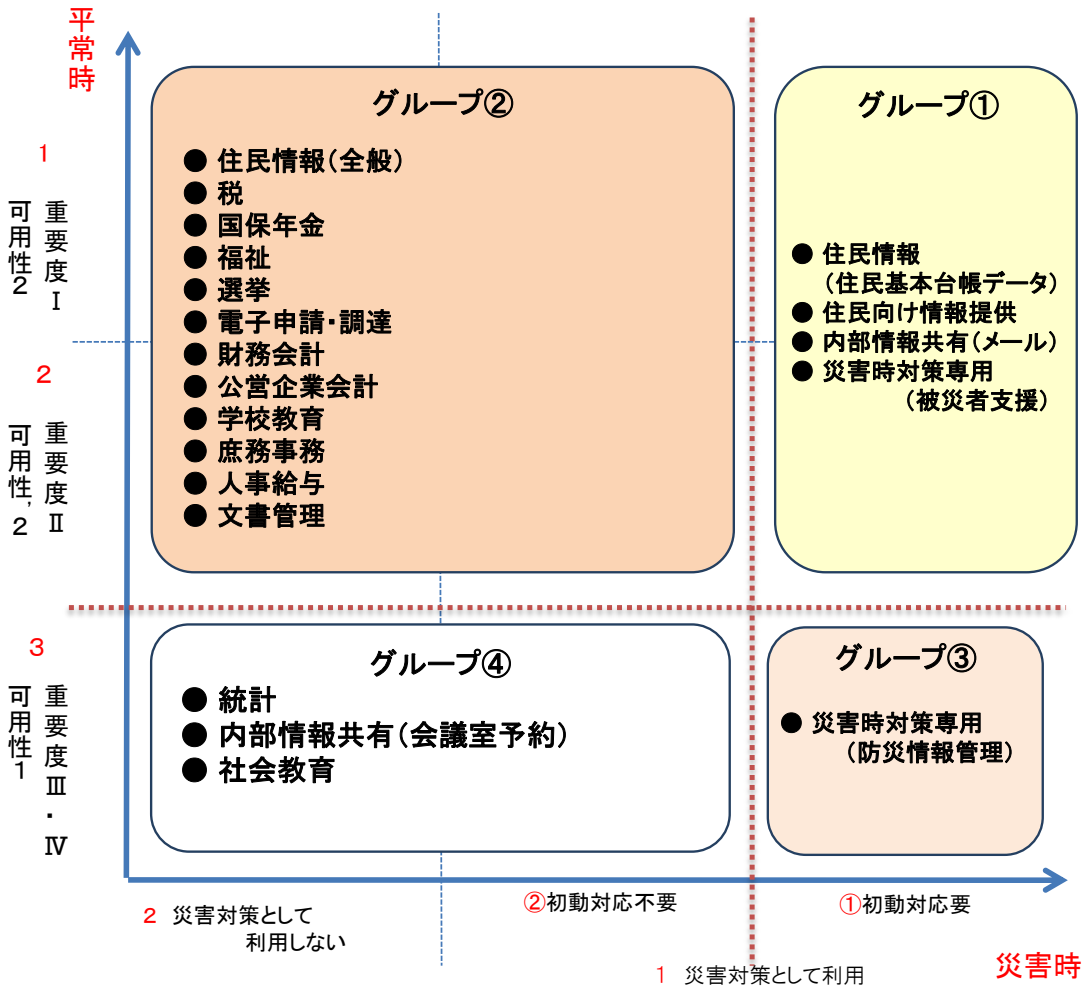
No	業務	情報システム例
1	税	県民税、自動車税、固定資産税　等
2	電子申請･調達	電子申請、電子調達、住民向け施設予約　等
3	財務会計	財務会計　等
4	上下水道	上下水道　等
5	学校教育	校務支援　等
6	土木積算	土木積算　等
7	庶務事務	勤怠管理、旅費管理　等
8	人事給与	人事給与　等
9	文書管理	公文書管理　等
10	統計	人口統計　等
11	住民向け情報提供	ホームページ、緊急通報　等
12	内部情報共有(メール)	メール　等
13	内部情報共有(会議室予約)	庁内会議室予約　等
14	災害時対策専用(被災者支援)	被災者支援、職員安否確認　等
15	災害時対策専用(防災情報管理)	災害情報収集、防災対策情報共有　等
16	社会教育	図書管理、web 予約、蔵書検索　等

対象とした市町村の業務及び情報システム例を表－19 に示す。

表－19　対象とした市町村の業務及び情報システム例

No	業務	情報システム例
1	住民情報(全般)	住民記録、印鑑登録、戸籍　等
2	住民情報(住民基本台帳データ)	住民基本台帳データ参照･出力　等
3	税	市町村税、法人税、軽自動車税　等
4	国保･年金	国民健康保険、国民年金　等
5	福祉	高齢者福祉、乳幼児医療　等
6	選挙	選挙人名簿、期日前投票　等
7	電子申請･調達	電子申請、電子調達、住民向け施設予約　等
8	財務会計	財務会計、上下水道会計　等
9	土木積算	土木積算　等
10	上下水道	上下水道　等
11	学校教育	校務支援、学齢簿　等
12	庶務事務	勤怠管理、旅費管理　等
13	人事給与	人事給与　等
14	文書管理	公文書管理
15	統計	人口統計　等
16	住民向け情報提供	ホームページ、緊急通報　等
17	内部情報共有(メール)	メール　等
18	内部情報共有(会議室予約)	庁内会議室予約　等
19	災害時対策専用(被災者支援)	被災者支援、職員安否確認　等
20	災害時対策専用(防災情報管理)	災害情報収集、防災対策情報共有　等
21	社会教育	図書管理、web 予約、蔵書検索　等

都道府県と市町村の業務を統合した情報システムの分類結果を図－17 に示す。この結果を基に、活用シートのとおり非機能要求グレードを定めている。



図－17　地方公共団体における業務・情報システム分類

なお、アンケートの回答においても、各地方公共団体によって意見が分かれるケースが多々発生しており、すべての地方公共団体が、上記の分類に従うことを求めるものではない。上記の分類を参考とし、地方公共団体ごとに最適な業務・情報システム分類を実施することが望ましい。

第５章 今後の展望と課題

非機能要求グレード（地方公共団体版）が、地方公共団体の情報システム調達においてより有効に活用され、その情報システムの適切な開発、安定的な運用を推進するための課題として、以下のような点が挙げられる。

第１節 環境変化への対応

ICT 分野における技術の発展は日進月歩であり、新たな製品の登場により非機能要件の実現が容易になる、あるいは、より低い費用で要件が実現可能となることも考えられる。また、IPA においては、非機能要求グレードの見直しを実施しているところである。なお、災害対策やセキュリティ等の分野については、社会的な要求・動向等にも影響を受ける。特に、総務省から公開されている「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」「ICT 部門の業務継続計画＜初動版解説書＞」「地方公共団体における情報セキュリティポリシーに関するガイドライン」「地方公共団体における情報セキュリティ監査に関するガイドライン」といった各種ガイドラインの改訂等にも注視する必要がある。さらに、今後クラウドサービスの高度化が進むことが見込まれるため「地方公共団体における ASP･SaaS 導入活用ガイドライン」の改訂にも注視していく。

非機能要求グレード（地方公共団体版）についても、これらの外部動向を把握しながら必要に応じ見直しを行っていく。

第２節 非機能要求グレード（地方公共団体版）の普及促進

今後、非機能要求グレード（地方公共団体版）を活用した事例等について、地方公共団体間で情報交換を行うことにより、その利用方法のノウハウと併せて共有されれば、その普及促進と有効活用の推進につながるものと考える。

なお、非機能要求グレード（地方公共団体版）の普及促進に当たり、当センターでは以下の活動を予定している。

・会員団体へのメールマガジンによる周知
・機関誌への記事掲載
・当センターのホームページへの掲載
・セミナーでの紹介
・研修の開催

特に、当センターホームページについては、IPA の非機能要求グレードのホームページ等、関連するホームページと相互にリンクを作成するといった働きかけを実施していくことにより、その存在をアピールし、参照契機を増加させるように努めていく。

また、非機能要求グレード（地方公共団体版）を有効に活用した団体の優良事例等をセミナー・ホームページ等で紹介していくことも検討していく。

先述した外部動向に応じた見直しに加え、上記の地方公共団体との情報交換により得られた意見・要望等を集約・分析し、妥当性のある意見は汲み取り、PDCA サイクルに従って非機能要求グレード（地方公共団体版）に反映し、地方公共団体にとってより利用しやすいツールとして成長させていく仕組み作りも検討する。

最終的にはこの非機能要求グレード（地方公共団体版）が地方公共団体における調達の非機能要求仕様に関しての標準的な参照先となることを目標とする。

第３節 情報システム調達手法全体の標準化

非機能要求グレード（地方公共団体版）は、情報システム調達仕様書に記載する内容をすべて網羅し解説しているわけではない。非機能要求グレード（地方公共団体版）を含む、情報システム調達仕様書全体の作成を支援する標準的なツールが整備されれば有益と考える。非機能要件以外の分野に関しても、様々な団体で検討会・調査研究が進められており、これらの成果を非機能要求グレード（地方公共団体版）と併せて、統合的に活用することにより、情報システム調達仕様書に関する情報網羅性を高めることができる。

例として、本調査研究と同時期に進められている「電子自治体の取組みを加速するための検討会」（総務省）[8]がある。この中で本調査研究では盛り込まなかった業務標準化推進及び SLA に関する検討が進められており、これらの成果を非機能要求グレード（地方公共団体版）と併せて活用することで、地方公共団体における情報システム調達仕様書作成の標準化がさらに進んでいくものといえる。

さらに、IPA において作成している「技術参照モデル（TRM：Technical Reference Model）」がある。TRM においては地方公共団体の調達ガイド作成に向けても取り組んでおり、平成 25 年度においては地方公共団体の実際の調達についての課題を整理し、その課題を解決するための方法をリファレンスモデルとして整備しているところである。そのうち非機能要件については非機能要求グレード（地方公共団体版）をそのまま使用することも想定しており、その意味では相互に補完しあうような関係と考えられる。

非機能要求グレード（地方公共団体版）では、ネットワーク要件・ファシリティ要件については個別の情報システム調達では実施しないことから対象外としているが、データセンターを利用する場合や、クラウドサービスを利用する場合はこれらの要件を記載することがある。クラウドサービスについては、今後さらなる普及が見込まれることから、何らかの形でのフォローも検討が必要である。

今後は、様々な団体において作成しているガイドライン等と、相互に補完しあう関係を強化していくとともに、最終的には地方公共団体向けの情報システム調達仕様書作成ガイドラインとして統合されることが望まれる。

---

[8] 総務省「電子自治体の取組みを加速するための検討会」 <http://www.soumu.go.jp/main_sosiki/kenkyu/denshijiti-kasoku/index.html>(最終アクセス 2014 年 2 月 4 日)。

【参考資料１】業務・情報システムアンケートについて

地方公共団体の業務・情報システムが、本調査で定義した 4 つのグループ①~④のいずれに属するか決定するために、アンケートを実施している。

アンケート結果の詳細について以下に紹介する。

1　都道府県アンケート結果

アンケート調査を A 団体及びオブザーバー（E 社、F 社、G 社）に対して実施した。（調査に使用した調査票については、調査票 1.「都道府県の業務・情報システム分類に対するアンケート調査票」を参照のこと。）

アンケートの回答及び回答結果を基にした調整結果を表－20 に示す。

表－20　都道府県アンケート結果

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
税	県民税 事業税 自動車税 等	A 団体	C	②	・個人情報の部類に属するが、災害時には利用はしないと思われる。	回答はすべてグループ②	グループ②	個人情報等、重要情報を扱う業務であるが、災害初動対応に必要な業務ではないため。
		E 社	C	②	・平常時の社会システムとして重要であるが、災害時には利用しない。平常時への復旧過程で一部の証明発行の早期再開が必要されることがある。			
		F 社	C	②	・災害対策には不要。復旧段階で権利関係等の証明に利用される可能性あり。データ消失は避ける必要あり。			
		G 社	B	②	・個人情報を取り扱う。証明書発行は、早期復旧が必要（証明書発行システムが独立していれば、必要なし）。			
電子申請・調達	電子申請 電子調達 住民向け施設予約　等	A 団体	C	②	・情報資産が利用できないことにより住民の権利が侵害されるが、災害時には利用しない又は利用しなくてもよい。	回答はグループ②と④に分かれるが、②が多い。	グループ②	個人情報等、重要情報を扱うが、災害初動対応に必要な業務ではないため。

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	E 電子申請・調達 F 住民向け施設予約	② ④	・電子申請・電子調達は、災害時には利用しないが、電子調達は復旧工事等で再開が望まれるケースがある。電子申請は業務呼称ではないが、申請対象業務によっては災害復旧時の早い段階で必要になる可能性が考えられる。住民向け施設予約は、災害時に使用しないのが一般的である。			
		F 社	F 電子申請・調達 H 住民向け施設予約	②	・災害対応には不要。電子調達の早期復旧が復旧段階の助けとなる可能性はあるが、優先度は低い。			
		G 社	F	②	・住民向けの利便性向上ツールであり、災害時には利用しない（代替手段がある）。			
財務会計	財務会計 土木積算 等	A 団体	E	②	・セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害直後には利用出来なくても仕方ないが、早期の復旧が必要。	回答はすべてグループ②	グループ②	庁内の重要情報を扱うが、災害初動対応に必要な業務ではないため。
		E 社	F 財務会計 E 土木積算	②	・財務会計は災害時には利用しない。 ・土木積算は災害時には利用しないが、通常の積算による復旧工事が開始される頃には利用が必要となることがある。			
		F 社	E	②	・初動には共に不要。財務会計は予算執行の迅速化のためにも早い復旧が望まれる。			
		G 社	E	②	・重要な行政事務であり、安定的な遂行が必要。災害直後には必ずしも利用しないが、比較的早期な復旧が求められる。			
学校教育	校務支援 等	A 団体	F	②	・セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害時には利用しない又は利用しなくてもよい。	回答はグループ②と④に分かれるが、②が多い。	グループ②	個人情報等の重要情報を扱う業務であるが、災害初動対応に必要な業務ではないため。
		E 社	I	④	・災害時には利用しない。復旧優先度も低い。			
		F 社	E	②	・災害時には利用しない。データの喪失はできるだけ避けるべき。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。普及要求は小さいと想定される。			
庶務事務	勤怠管理 旅費管理 等	A 団体	E	②	・セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害直後には利用出来なくても仕方ないが、早期の復旧が必要。	回答はグループ②と④に分かれるが、②が多い。	グループ②	市民生活への影響度はそれほど大きくないが、行政事務の円滑な運営に必要な業務である。災害初動対応に必要な業務ではない。

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	I	④	・災害時には利用しない。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。復旧要求は小さいと想定される。			
人事給与	人事 給与　等	A 団体	C	②	・個人情報の部類に属するが、災害時には利用はしないと思われる。	回答はすべてグループ②	グループ②	地方公共団体職員の個人情報等の重要情報を扱う業務であるが、災害初動対応に必要な業務ではない。
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	F	②	・災害時には利用しない。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。復旧要求は小さいと想定される。			
文書管理	公文書管理 電子決済 等	A 団体	F 公文書管理 E 電子決済 等	②	＜公文書管理＞セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害時には利用しない又は利用しなくてもよい。 ＜電子決済＞セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害直後には利用出来なくても仕方ないが、早期の復旧が必要。	回答はすべてグループ②	グループ②	庁内の重要情報を扱う業務であるが、災害初動対応に必要な業務ではないため。
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	F	②	・災害時には利用しない。文書管理に関するデータの保全は必要。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない(代替手段がある)。			
統計	人口統計 等	A 団体	I	④	・公開しているものが多く、セキュリティ侵害があったとしても行政事務の執行への影響は小さく、災害直後には利用出来なくてもよい。	回答はすべてグループ④	グループ④	個人情報等、重要情報を扱わず、災害初動対応に必要な業務ではないため。
		E 社	I	④	・元々優先度の低い業務であり、災害時にも利用しない。			
		F 社	I	④	・災害時には利用しない。データが喪失しても被害は少ないと想定される。			
		G 社	I	④	・個人情報が含まれない統計情報を扱う。災害時には利用しない。			
住民向け情報提供	ホームページ 緊急通報 等	A 団体	G	③	・公開しているものが多く、セキュリティ侵害があったとしても行政事務の執行への影響は小さく、災害直後には利用出来なくてもよい。	回答はグループ①、③、④に分かれている。	グループ③	平常時、災害時の情報発信等に利用される業務であるが、利用する情報は公開しているものが多い。また、災害時に即時必要とされる業務のため。

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	D	①	・元々優先度の低い業務であり、災害時にも利用しない。			
		F 社	D	①	・災害時には利用しない。データが喪失しても被害は少ないと想定される。			
		G 社	I ホームページ G 緊急通報	④ ③	＜ホームページ＞ 公開情報であり、災害時には利用しない(代替手段がある)。 ＜緊急情報、災害時情報提供＞ 災害時に住民への情報提供手段として極めて重要である。			
内部情報共有	メール 会議室予約等	A 団体	D メール E 会議室予約等	① ②	＜メール＞セキュリティ侵害が行政事務の執行に重大な影響を及ぼし、災害直後速やかに利用出来なくてはならないシステム。 ＜会議室予約＞セキュリティ侵害が行政事務の執行に重大な影響を及ぼすが、災害直後には利用出来なくても仕方ないが、早期の復旧が必要。	回答は①、②、③、④で分かれている。	内部情報共有(メール)については、グループ①に分類する。 内部情報共有(会議室予約)については、グループ④に分類する。	メールについて平常時、災害時の情報連絡ツールとして重要度が高く、災害時に即時利用される業務であるため、グループ①に分類する。 会議室予約については、職員のみが利用するツールであり、システム停止による市民生活への影響がない。また、災害時の即時復旧は必要なく、復旧の優先順位も低いためグループ④に分類する。
		E 社	G メール I 会議室予約	③ ④	・「メール」を災害時に職員の緊急連絡として活用する場合には、可能な限り早期の利用が必要となる。			
		F 社	G メール I 会議室予約	③ ④	・外部との連絡に際しても電子メールが有効に機能する場合が考えられ、早急な復旧が望まれる。			
		G 社	G メール I 会議室予約	③ ④	＜会議室予約＞ 職員向けのツールであり、災害時には利用しない(代替手段がある)。 ＜メール(緊急連絡)＞ 災害時に職員間の情報連絡手段として極めて重要である。			
災害時対策専用	被災者支援 防災情報管理 等	A 団体	A	①	・個人情報の部類に属し、災害直後速やかに利用出来なくてはならないシステム。	回答は①、③、④で分かれている。	被災者支援についてはグループ①に分類する。 防災情報管理についてはグループ③に分類する。	被災者支援については、災害時に重要情報を扱う業務であり、災害時に即時利用される業務であるため、グループ①に分類する。 防災情報管理については、重要情報を扱う業務ではないが、災害時の情報収集等で即時必要とされる業務であるため、グループ③に分類する。
		E 社	D 被災者支援	①	・災害時に利用する重要システムであり、可能な限り早期の利用が必要となる。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		F社	D 被災者支援 H 防災情報管理	① ④	・被災者支援の一部（避難所管理等）は初動から利用可能であることが望まれる。り災証明などは復旧後でよい。			
		G社	A 被災者支援 G 防災情報管理	① ③	＜被災者支援＞重要な住民個人情報を取り扱う。災害直後に、利用されるシステムの為、極めて重要である。 ＜防災情報管理＞ センシティブな個人情報は含まれない。主に、災害時に利用されるシステムであり、災害時の安定した行政事務の遂行が必要である。			
社会教育	図書館 博物館管理 生涯学習支援 等	A団体	I	④	・公開しているものが多く、セキュリティ侵害があったとしても行政事務の執行への影響は小さく、災害直後には利用出来なくてもよい。	回答はすべてグループ④	グループ④	社会教育については個人情報等、重要情報を扱わず、災害初動対応に必要な業務ではないためグループ④に分類する。
		E社	I	④	・災害時には利用しない。復旧優先度も低い。			
		F社	I	④	・災害時には利用しない。			
		G社	I	④	・住民向けの利便性向上のツールであるが、災害時には利用しない。復旧要求は小さいと想定される。センシティブな個人情報は含まれない。			

2　市町村アンケート結果

アンケート調査をB団体、C団体、D団体及びオブザーバー（E社、F社、G社）に対して実施した。（調査に使用した調査票については、調査票2.「市町村の業務・情報システム分類に対するアンケート調査票」を参照。）

アンケートの回答及び回答結果を基にした調整結果を表－21に示す。

表－21　市町村アンケート結果

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
住民情報	住民記録 印鑑登録 戸籍 住登外管理 等	B団体	A	①	・市の根幹となる業務システムで代替えがないものの中で災害時のRTOが短時間の業務。	回答は①、②で分かれている。	・住民情報（住民基本台帳データ）を①に分類する。 ・住民情報（全般）を②に分類する。	住民基本台帳データは個人情報等、重要情報を扱う業務であり、災害初動期に必要となる。住民基本台帳データ以外については、個人情報を扱い市民生活への影響が大きい業務であるが、災害初動対応に必要な業務ではない。
		C団体	A	①	・市民生活への影響が大きいため平常時の重要度は高い。災害時に基本4情報（氏名、生年月日、性別、住所）や世帯情報の確認に使用することを想定しているため、災害直後から必要。			
		D団体	B	②	・個人情報等を扱い、可用性、重要性ともに高いシステム。災害初動対応時に災害対応システム（被災者支援システム等）で必要とされるのは住記データなどの情報。これらのデータが利用可能な機能（台帳出力、二次加工可能なデータ等）を有していれば、システム自体は「初動対応不要」のレベルと考えられる。また、運用面などを考慮すると、税、国保、福祉などとともに「基幹業務システム」として一体のグループで扱うべきと考える。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	B	②	・平常時の社会システムとして重要であるが、災害時には利用しない。激甚災害等社会インフラ停止状態の利用は想定していないが、平常時への復旧過程で、証明書発行の早期再開が必要となる。なお将来的に、住民基本台帳データを被災者管理システムに利用する場合は、災害直後のデータ抽出が必要になるが、大規模災害等では市町村システムのデータから直接抽出するのではなく、堅牢なデータセンターのバックアップデータから抽出する可能性を想定すべきと思われる。			
		F 社	A	①	・災害対応には不要。復旧段階で権利関係等の証明に利用される可能性あり。データの消失は避ける必要あり。			
		G 社	B	②	・重要な住民個人情報を取り扱う。証明書発行は、早期復旧が必要（証明書発行システムが独立していれば、必要なし）。			
税	個人住民税 法人税 軽自動車税 固定資産税 等	B 団体	B	②	・市の根幹となる業務システムで代替えがないものの中で災害時の RTO が中時間の業務。	回答はすべてグループ②	グループ②	個人情報等、重要情報を扱い市民生活への影響が大きい業務であるが、災害初動対応に必要ないため。
		C 団体	B	②	・市民生活への影響が大きいため平常時の重要度は高い。災害時にり災証明を出す際、家屋情報の確認に使用することを想定。家屋情報以外の税情報は「C」でもよいかもしれないが、税総合システムとして導入されるケースが多いため「B」とするもの。災害対策には必要だが、災害直後には必要ない。			
		D 団体	B	②	・個人情報等を扱い、可用性、重要性ともに高いシステム。災害初動対応時に災害対応システム（被災者支援システム等）で必要とされるのはり災証明書発行等に関わるデータ。これらのデータが利用可能な機能（台帳出力、二次加工可能なデータ等）を有していれば、システム自体は「初動対応不要」のレベルと考えられる。 また、運用面などを考慮すると、税、国保、福祉などとともに「基幹業務システム」として一体のグループで扱うべきと考える。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	C	②	・平常時の社会システムとして重要であるが、災害時には利用しない。平常時への復旧過程で、所得証明等の一部の証明発行の早期再開が必要となる。			
		F 社	C	②	・初動には不要。復旧段階で所得証明などの出力が望まれる。			
		G 社	B	②	・重要な住民個人情報を取り扱う。証明書発行は、早期復旧が必要（証明書発行システムが独立していれば、必要なし）。			
国保年金	国民健康保険 国民年金等	B 団体	C	②	・市民生活への影響が大きいため平常時の重要度は高いが、災害対策としては必要ない。	回答はグループ①と②に分かれるが、②が多い。	グループ②	個人情報を扱い市民生活への影響が大きい業務であるが、災害初動対応に必要な業務ではないため、グループ②に分類する。
		C 団体	E	②	・市の根幹となる業務システムで代替えがないものの中で災害時に最低限の市民生活を営むために必要な業務。			
		D 団体	B 国保 F 年金	②	＜国保＞個人情報等を扱い、可用性、重要性ともに高いシステム。災害初動対応時に災害対応システム（被災者支援システム等）等で必要とされるのは保険証、レセプト等に関わるデータ。これらのデータが利用可能な機能（台帳出力、二次加工可能なデータ等）を有していれば、システム自体は「初動対応不要」のレベルと考えられる。 また、運用面などを考慮すると、税、国保、福祉などとともに「基幹業務システム」として一体のグループで扱うべきと考える。 ＜年金＞年金に関するデータ等の主幹団体は「日本年金機構」。市町村は提供されるデータを基に申請受付、相談業務等を行う。そのためシステムの重要性や災害時対応などは、国保などの基幹業務システムに比べ１段階ずつ低くなると考えられる。			
		E 社	C	②	・平常時の社会システムとして重要であるが、災害時には利用しない。平常時への復旧過程で、国保被保険者賞等の一部の証明書発行の早期再開が必要となる。			
		F 社	A	①	・初動には不要。復旧段階で被保険者章などの資格関連証明書の出力が望まれる。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		G 社	B	②	・重要な住民個人情報を取り扱う。証明書発行は、早期復旧が必要（証明書発行システムが独立していれば、必要なし）。			
福祉	高齢者福祉 障がい者福祉 乳幼児医療 健康管理 等	B 団体	E	②	・市の根幹となる業務システムで代替えがないものの中で災害時に最低限の市民生活を営むために必要な業務。	回答はグループ①と②に分かれるが、②が多い。	グループ②	個人情報を扱い市民生活への影響が大きい業務であるが、災害初動対応に必要な業務ではないため。
		C 団体	A	①	・市民生活への影響が大きいため平常時の重要度は高い。災害時に高齢者や障害者情報の確認に使用することを想定しているため、災害直後から必要。			
		D 団体	B	②	・個人情報等を扱い、可用性、重要性ともに高いシステム。災害初動対応時に災害対応システム（被災者支援システム等）で必要とされるのは災害弱者等に関わるデータ。これらのデータが利用可能な機能（台帳出力、二次加工可能なデータ等）を有していれば、システム自体は「初動対応不要」のレベルと考えられる。 また、運用面などを考慮すると、税、国保、福祉などとともに「基幹業務システム」として一体のグループで扱うべきと考える。			
		E 社	C	②	・平常時の社会システムとして重要であるが、災害時には利用しない。平常時の復旧過程で一部証明書が必要とされる場合がある。			
		F 社	B	②	・業務自体は初動には不要であるが、要救助対象の特定等、データは初動段階で参照が望まれる。			
		G 社	B	②	・重要な住民個人情報を取り扱う。証明書発行は、早期復旧が必要（証明書発行システムが独立していれば、必要なし）。			
選挙	選挙人名簿 期日前投票 等	B 団体	I	④	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が長時間の業務。	回答はグループ②と④に分かれるが、②が多い。	グループ②	個人情報を扱い市民生活への影響が大きい業務であるが、災害初動対応に必要な業務ではないため。
		C 団体	C	②	・市民生活への影響が大きいため平常時（選挙期間中）の重要度は高いが、災害対策としては必要ない。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		D 団体	F	②	・選挙期間中の利用を想定。（選挙が予定されていない場合は、Iグループでよいと考える。） 住民の権利に関わる業務ではあるが、システム停止時の代替手段も確保されているため、影響は小さい。			
		E 社	C	②	・平常時の社会システムとして重要であるが、災害時には利用しない。			
		F 社	F	②	・災害時には利用しない。			
		G 社	C	②	・重要な住民個人情報を取り扱う。災害時には利用しない。			
電子申請・ 調達	電子申請 電子調達 住民向け施設予約　等	B 団体	E	②	・市の根幹となる業務システムで代替えがないものの中で災害時に最低限の市民生活を営むために必要な業務。	回答はグループ②と④に分かれるが、②が多い。	グループ②	重要情報を扱い、行政業務の円滑な執行、市民サービス向上等に必要な業務であるが、災害初動対応に必要な業務ではないため、グループ②に分類する。
		C 団体	C	②	・市民生活への影響が大きいため平常時の重要度は高いが、災害対策としては必要ない。			
		D 団体	F	②	・市民サービスの利便性を向上させる手段であり、安定的な執行が求められる。災害時は代替手段などにより執行が可能。 なお、電子入札などの調達に関しても、災害時は紙文書による手続きが行われることや入札ではなく随意契約がおこなわれると想定できる。			
		E 社	E 電子申請・調達 F 住民向け施設予約	②	・電子申請・電子調達は、災害時には利用しないが、電子調達は復旧工事等で再開が望まれるケースがある。電子申請は業務呼称ではないが、申請対象業務によっては災害復旧時の早い段階で必要になる可能性が考えられる。 住民向け施設予約は、災害時に使用しないのが一般的である。			
		F 社	F 電子申請・調達 H 住民向け施設予約	② ④	・災害対応には不要。電子調達の早期復旧が復旧段階の助けとなる可能性はあるが、優先度は低い。			
		G 社	F	②	・住民向けの利便性向上ツールであり、災害時には利用しない(代替手段がある)。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
財務会計	財務会計 土木積算 等	B 団体	B	②	・市の根幹となる業務システムで代替えがないものの中で災害時の RTO が中時間の業務。	回答はすべてグループ②	グループ②	重要情報を扱い、行政業務として重要であるが、災害初動対応に必要な業務ではないため。
		C 団体	E	②	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害対策には必要だが、災害直後には必要ない。			
		D 団体	E	②	・事務全般に関わる手続きであり、安定的な執行が求められる。災害時には緊急の物資購入などのため財務執行が求められることから、初動後の対応としてシステム利用が想定される。			
		E 社	F 財務会計 E 土木積算	②	・財務会計は災害時には利用しない。 ・土木積算は災害時には利用しないが、通常の積算による復旧工事が開始される頃には利用が必要となることがある。			
		F 社	E	②	・初動には共に不要。財務会計は予算執行の迅速化のためにも早い復旧が望まれる。			
		G 社	E	②	・重要な行政業務であり、安定的な遂行が必要。			
公営企業会計	上下水道料金　等	B 団体	E	②	・市の根幹となる業務システムで代替えがないものの中で災害時に最低限の市民生活を営むために必要な業務。	回答はすべてグループ②	グループ②	重要情報を扱い、市民生活への影響が大きい行政業務であるが、災害初動対応に必要な業務ではないため。
		C 団体	C	②	・市民生活への影響が大きいため平常時の重要度は高いが、災害対策としては必要ない。			
		D 団体	E	②	・料金に関わる手続きであり、安定的な執行が求められる。財務会計と同様、初動後の対応としてシステム利用が想定される。			
		E 社	F 上下水道料金 F 公営企業会計	②	・上下水道料金は災害時には利用しない。			
		F 社	F	②	・災害時には利用しない。			
		G 社	E	②	・重要な行政事務であり、安定的な遂行が必要。災害直後には必ずしも利用しないが、比較的早期な復旧が求められる。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
学校教育	校務支援 学齢簿　等	B 団体	E	②	・市の根幹となる業務システムで代替えがないものの中で災害時に最低限の市民生活を営むために必要な業務。	回答はグループ②と④に分かれるが、②が多い。	グループ②	個人情報等の重要情報を扱う業務であるが、災害初動対応に必要な業務ではないため。
		C 団体	E	②	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害対策には必要だが、災害直後には必要ない。			
		D 団体	E	②	・児童生徒の情報を取り扱うため、安定的な執行が求められるとともに、災害時には名簿情報等が必要とされるため、影響は大きい。			
		E 社	I	④	・災害時には利用しない。復旧優先度も低い。			
		F 社	I	④	・災害時には利用しない。データの喪失はできるだけ避けるべき。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。復旧要求は小さいと想定される。			
庶務事務	勤怠管理 旅費管理 等	B 団体	I	④	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が長時間の業務。	回答はグループ①、②、④に分かれるが、②が多い。	グループ②	市民生活への影響度はそれほど大きくなく、行政事務の円滑な運営に必要な業務であるが、災害初動対応に必要な業務ではないため、グループ②に分類する。なお、庶務事務システムを安否確認に活用するケースは必ずしも一般的でないと考えた。
		C 団体	D	①	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害時に職員の安否確認に使用することを想定しているため、災害直後から必要。			
		D 団体	F	②	・職員の事務手続き等の利便性を向上させる手段ではあり、安定的な執行が求められる。災害時は代替手段などにより執行が可能。			
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	I	④	・災害時には利用しない。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。復旧要求は小さいと想定される。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
人事給与	人事 給与　等	B 団体	I	④	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が長時間の業務。	回答はグループ②、④に分かれるが、②が多い。	グループ②	自治体職員の個人情報を扱う業務であり業務の重要性は高いが、災害初動対応に必要な業務ではないため。
		C 団体	F	②	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害対策としては必要ない。※職員情報が人事給与システムで管理されている場合は、災害時に職員の安否確認に使用するため「D」とする。			
		D 団体	E	②	・職員の個人情報等を含む手続きであり、安定的な執行が求められる。災害時も職員への給与支給などの対応は求められると考えられることから、初動後の対応としてシステム利用が想定される。			
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	F	②	・災害時には利用しない。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない。復旧要求は小さいと想定される。			
文書管理	公文書管理 電子決済 等	B 団体	F	②	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が中時間の業務。	回答はすべてグループ②	グループ②	庁内の重要情報を扱う業務であるが、災害初動対応に必要な業務ではないため。
		C 団体	F	②	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害対策としては必要ない。			
		D 団体	F	②	・職員の事務手続き等の利便性を向上させる手段であり、安定的な執行が求められる。災害時は代替手段などにより執行が可能。			
		E 社	F	②	・災害時には利用しない。復旧優先度も低い。			
		F 社	F	②	・災害時には利用しない。文書管理に関するデータの保全は必要。			
		G 社	F	②	・重要な行政事務であり、安定的な遂行が必要。災害時には利用しない(代替手段がある)。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
統計	人口統計等	B 団体	I	④	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が長時間の業務 。	回答はすべてグループ④	グループ④	個人情報等、重要情報を扱う業務ではなく、災害初動対応に必要な業務ではないため。
		C 団体	I	④	・市民生活への影響は小さいため平常時の重要度は低い。災害対策としては必要ない。			
		D 団体	I	④	・個人情報等が含まれない統計情報であり、システム停止等による影響は少ない。			
		E 社	I	④	・元々優先度の低い業務であり、災害時にも利用しない。			
		F 社	I	④	・災害時には利用しない。データが喪失しても被害は少ないと想定される。			
		G 社	I	④	・個人情報が含まれない統計情報を扱う。災害時には利用しない。			
住民向け情報提供	住民向け情報提供	B 団体	A	①	・市の根幹となる業務システムで代替えがないものの中で災害時の RTO が短時間の業務。	回答はグループ①、③、④に分かれている。	グループ①	公開情報を扱う業務ではあるが、平常時、災害時の情報発信等、市民に与える影響は大きい。また、災害時に即時必要とされる業務のため。 総務省「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」「ICT 部門の業務継続計画＜初動版解説書＞でも、初動対応業務として、「⑥避難所、住民、外部に対する情報提供（収集した住民の安否情報などを地域内外にインターネットを始めとする様々な手段で、安否情報、被害状況などの被災地関連の情報提供を行う）」を挙げている。
		C 団体	A	①	・市民生活への影響が大きいため平常時の重要度は高い。災害時は情報発信のツールとして使用することを想定しているため、災害直後から必要。			
		D 団体	D	①	・公開情報ではあるが、改ざん等による影響は大きい。災害時にも住民に必要な情報を提供する環境であることから影響は大きい。 なお、情報提供・発信の手段として、HPの他に、防災行政無線、エリアメール、公共情報コモンズなども想定される。			
		E 社	D 緊急通報	①	・「緊急通報システム」を災害時に住民向けの緊急連絡として活用する場合には、可能な限り早期の利用が必要となる。			
		F 社	D	①	・ホームページに関しては、初動段階以降アクセスの集中などが考えられ、ミラーサイト設置など平時以上の対応が必要。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		G 社	I ホームページ G 緊急通報	④ ③	＜ホームページ＞ 公開情報であり、災害時には利用しない(代替手段がある)。 ＜緊急情報、災害時情報提供＞ 災害時に住民への情報提供手段として極めて重要である。			
内部情報共有	メール 会議室予約等	B 団体	A	①	・市の根幹となる業務システムで代替えがないものの中で災害時の RTO が短時間の業務。	回答はグループ①、③、④に分かれている。	メールについてはグループ①に分類する。 会議室予約についてはグループ④に分類する。	・メールについては、平常時、災害時の情報連絡ツールとして重要度が高く、災害時に即時利用される業務であるため。 ・会議室予約については、職員のみが利用するツールであり、システム停止による市民生活への影響がなく、災害時の即時復旧は必要なく、復旧の優先順位も低いため。
		C 団体	D	①	・市民生活への影響はそれほど大きくないが行政事務としては重要であるため、平常時の重要度は中。災害直後から必要。※当市の現状にはそぐわないが、災害時に職員間連携ツールとして積極的に活用すべきと考えられるため「D」とするもの。			
		D 団体	D メール I 会議室予約	① ④	＜メール＞日常的にも非常時にも重要な情報共有ツールであり、システム停止等による影響は大きい。 ＜会議室予約等＞職員の事務手続き等の利便性を向上させる手段ではあるが、代替手段が確保されている等の理由から影響は少ない。			
		E 社	G メール I 会議室予約	③ ④	・「メール」を災害時に職員の緊急連絡として活用する場合には、可能な限り早期の利用が必要となる。			
		F 社	G メール I 会議室予約	③ ④	・外部との連絡に際しても電子メールが有効に機能する場合が考えられ、早急な復旧が望まれる。			
		G 社	G メール I 会議室予約	③ ④	＜メール(緊急連絡)＞ 災害時に職員間の情報連絡手段として極めて重要である。 ＜会議室予約＞ 職員向けのツールであり、災害時には利用しない(代替手段がある)。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
災害時対策専用	被災者支援 防災情報管理	B 団体	A	①	・市の根幹となる業務システムで代替えがないものの中で災害時の RTO が短時間の業務。	回答はグループ①、③、④に分かれている。	・災害時対策専用（被災者支援）についてはグループ①に分類する。 ・災害時対策専用（防災情報管理）についてはグループ③に分類する。	・被災者支援は災害時のり災証明発行業務等により重要情報を扱い、災害時に即時利用される業務であるため。 ・防災情報管理は重要情報を扱う業務ではないが、災害時の情報収集等で即時必要とされる業務であるため。 ・防災情報管理は、より具体的に、システム例として災害情報収集、安否確認、防災対策情報共有とする。
		C 団体	G	③	・平常時はほぼ使用しない。災害直後から必要。			
		D 団体	G 情報収集 H 復興支援	③ ④	＜情報収集＞日常的に利用される頻度は少ないが、災害時には初動対応から使用することが想定されるものである。 被害状況把握やテレビ会議、安否確認など、情報収集に関する業務が中心。インターネット環境を利用したシステム等が多く含まれると想定される。 ＜復興支援＞日常的に利用される頻度は少ないが、災害時には初動後の対応として使用することが想定されるものである。被災者支援システムや工事契約管理システムなど、災害復興期に必要とされるシステムが想定される。			
		E 社	D 被災者支援	①	・災害時に利用する重要システムであり、可能な限り早期の利用が必要となる。			
		F 社	D 被災者支援 H 防災情報管理	① ④	・被災者支援の一部（避難所管理等）は初動から利用可能であることが望まれる。り災証明などは復旧後でよい。			
		G 社	A 被災者支援 G 防災情報管理	① ③	＜被災者支援＞　重要な住民個人情報を取り扱う。災害直後に、利用されるシステムの為、極めて重要である。 ＜防災情報管理＞　センシティブな個人情報は含まれない。主に、災害時に利用されるシステムであり、災害時の安定した行政事務の遂行が必要である。			
社会教育	図書館 博物館管理 障害学習支援	B 団体	I	④	・業務システム利用できない場合代替え手段で業務の継続は可能であるが大幅に効率が低下するものの中で災害時の RTO が長時間の業務。	回答はすべてグループ④	グループ④	社会教育については個人情報等、重要情報を扱わず、災害初動対応に必要な業務ではないため。
		C 団体	I	④	・市民生活への影響は小さいため平常時の重要度は低い。災害対策としては必要ない。			
		D 団体	I	④	・市民サービスの利便性を向上させる手段であるが、代替手段が確保されている等の理由から影響は少ない。			

アンケート回答						調整結果		
業務	システム例	回答者	分類ｸﾞﾙｰﾌﾟ		分類理由	回答傾向	結論	理由
			A～I	①～④				
		E 社	I	④	・災害時には利用しない。復旧優先度も低い。			
		F 社	I	④	・災害時には利用しない。			
		G 社	I	④	・住民向けの利便性向上のツールであるが、災害時には利用しない。復旧要求は小さいと想定される。センシティブな個人情報は含まれない。			

【参考資料２】グループごとの選択レベル比較

グループ①～④における選択レベルを比較表としたものを以下に示す。グループ①～④の選択レベルが異なる箇所を特定したい場合等は、表－22～24 を参照願う。

表－22　活用シート【Ｉ全庁的要求事項シート】における選択レベルの比較

項番	メトリクス（指標）	選択レベル							
		グループ①		グループ②		グループ③		グループ④	
C.1.2.2	外部データの利用可否	2	外部データは利用できない			1	一部のデータ復旧に利用できる		
C.2.3.5	OS パッチ適用タイミング	4	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う						
C.4.4.1	リモート監視地点	1	庁内 LAN を介してリモート監視を行う			0	リモート監視を行わない		
C.4.4.3	リモート操作時の接続方法	0	リモート操作を行わない						
E.1.1.1	順守すべき規程、ルール、法令、ガイドライン等の有無	1	有り						
E.2.1.1	リスク分析範囲	1	重要度が高い資産を扱う範囲、あるいは、外接部分			0	分析なし		
E.4.3.4	ウィルス定義ファイル適用タイミング	2	定義ファイルリリース時に実施						
E.5.1.1	管理権限を持つ主体の認証	1	1 回						
E.5.2.1	システム上の対策における操作制限度	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可						
E.6.1.1	伝送データの暗号化の有無	1	認証情報のみ暗号化						
E.6.1.2	蓄積データの暗号化の有無	1	認証情報のみ暗号化						
E.7.1.1	ログの取得	1	必要なログを取得する						
E.7.1.3	不正監視対象（装置）	1	重要度が高い資産を扱う範囲、あるいは、外接部分						
E.10.1.1	セキュアコーディング、Web サーバの設定等による対策の強化	1	対策の強化						
E.10.1.2	WAF の導入の有無	0	無し						
F.3.1.1	規格取得の有無（安全性）	1	規格取得の必要有り			0	規格取得の必要無し		
F.3.2.1	規格取得の有無（有害物質）	1	RoHS 指令相当取得			0	規格取得の必要無し		
F.5.1.1	グリーン購入法対応度	0	対処不要						

表－23　活用シート【Ⅱ業務主管部門要求事項シート】における選択レベルの比較

項番	メトリクス（指標）	選択レベル							
		グループ①		グループ②		グループ③		グループ④	
A.1.3.1	RPO（目標復旧地点）（業務停止時）	3	障害発生時点（日次バックアップ+アーカイブからの復旧）			1	5営業日前の時点（週次バックアップからの復旧）		
A.1.3.2	RTO（目標復旧時間）（業務停止時）	3	6時間以内					1	1営業日以内
A.1.3.3	RLO（目標復旧レベル）（業務停止時）	2	全システム機能の復旧			1	一部システム機能の復旧		
A.1.4.1	システム再開目標（大規模災害時）	4	3日以内に再開	2	一ヶ月以内に再開	4	3日以内に再開	1	数ヶ月以内に再開
A.1.5.1	稼働率	3	99.5%						
B.1.1.1	ユーザ数	1	上限が決まっている			0	特定ユーザのみ		
B.1.1.2	同時アクセス数	1	同時アクセスの上限が決まっている			0	特定利用者の限られたアクセスのみ		
B.1.1.3	データ量(項目・件数)	0	すべてのデータ量が明確である						
B.1.1.4	オンラインリクエスト件数	0	処理ごとにリクエスト件数が明確である						
B.1.1.5	バッチ処理件数	0	処理単位ごと毎に処理件数が決まっている						
B.1.2.1	ユーザ数増大率	1	1.2倍			0	1倍		
B.1.2.2	同時アクセス数増大率	1	1.2倍			0	1倍		
B.1.2.3	データ量増大率	1	1.2倍			0	1倍		
B.1.2.4	オンラインリクエスト件数増大率	1	1.2倍			0	1倍		
B.1.2.5	バッチ処理件数増大率	1	1.2倍			0	1倍		
B.2.1.4	通常時オンラインレスポンスタイム	3	3秒以内			0	規定しない		
B.2.1.5	アクセス集中時のオンラインレスポンスタイム	2	5秒以内			0	規定しない		
B.2.2.1	通常時バッチレスポンス順守度合い	2	再実行の余裕が確保できる			0	順守度合いを定めない		
B.2.2.2	アクセス集中時のバッチレスポンス順守度合い	2	再実行の余裕が確保できる			0	順守度合いを定めない		
C.1.1.1	運用時間（平日）	1	定時内での利用（1日8時間程度利用）						
C.1.1.2	運用時間（休日等）	0	規定無し（原則利用しない）						
C.1.2.5	バックアップ取得間隔	4	日次で取得			1	システム構成の変更時など、任意のタイミング		
C.3.3.1	対応可能時間	0	ベンダーの営業時間内（例：9時～17時）で対応を行う						

項番	メトリクス（指標）	選択レベル							
		グループ①		グループ②		グループ③		グループ④	
C.3.3.2	駆けつけ到着時間	4	保守員到着が異常検知から数時間内			3	保守員到着が異常検知からユーザの翌営業開始時まで		
C.3.3.4	障害検知通知時間	0	障害を検知しない						
C.4.3.1	マニュアル準備レベル	2	情報システムの通常運用と保守運用のマニュアルを提供する			0	各製品標準のマニュアルを利用する		
C.4.5.1	外部システムとの接続有無	1	庁内の外部システムと接続する			0	外部システムと接続しない		
C.5.1.2	保守契約（ハードウェア）の種類	4	定額保守（オンサイト）						
C.5.2.2	保守契約（ソフトウェア）の種類	2	アップデート			1	問合せ対応		
C.5.3.1	ライフサイクル期間	1	5 年						
C.5.5.1	一次対応役割分担	2	すべてベンダーが実施						
C.5.6.2	ベンダー側対応時間帯	1	ベンダーの定時時間内（9～17 時）						
D.1.1.2	システム停止可能日時	4	利用の少ない時間帯（夜間など）			1	5 日以上		
D.3.1.1	設備・機器の移行内容	3	移行対象設備・機器のシステム全部を入れ替える			0	移行対象無し		
D.4.1.1	移行データ量	2	10TB 未満			1	1TB 未満		
D.5.1.1	移行のユーザ/ベンダー作業分担	1	ユーザとベンダーと共同で実施						
F.1.1.1	構築時の制約条件	1	制約有り（重要な制約のみ適用）			0	制約無し		
F.1.2.1	運用時の制約条件	1	制約有り（重要な制約のみ適用）			0	制約無し		
F.2.2.1	クライアント数	1	上限が決まっている			0	特定クライアントのみ		
F.2.5.1	特定製品の採用有無	1	一部に特定製品の指定がある			0	特定製品の指定がない		

表－24　活用シート【Ⅲ実現方法要求事項シート】における選択レベルの比較

項番	メトリクス（指標）	選択レベル							
		グループ①		グループ②		グループ③		グループ④	
A.2.1.1	冗長化（サーバ機器）	2	すべてのサーバで冗長化	1	特定のサーバで冗長化			0	非冗長構成
A.2.5.1	冗長化（ストレージ機器）	2	すべての機器を冗長化	1	特定の機器のみ冗長化			0	非冗長構成
A.2.5.3	冗長化（ストレージのディスク）	1	RAID5 による冗長化						
A.3.1.1	復旧方針	3	限定された構成をDR サイトで構築	2	同一の構成で情報システムを再構築	3	限定された構成をDR サイトで構築	2	同一の構成で情報システムを再構築

項番	メトリクス（指標）	選択レベル							
		グループ①		グループ②		グループ③		グループ④	
A.3.2.1	保管場所分散度（外部保管データ）	2	1ヵ所(遠隔地)			1	1ヵ所(近隣の別な建物)		
A.3.2.2	保管方法（外部保管データ）	2	DRサイトへのリモートバックアップ	0	媒体による保管				
B.1.3.1	保管期間（データ）	3	5年			1	1年		
C.1.2.3	データ復旧の対応範囲	1	障害発生時のデータ損失防止						
C.1.2.4	バックアップ自動化の範囲	2	1ステップのみ手動で行う（外部媒体交換のみ）						
C.1.3.1	監視情報	3	エラー監視（トレース情報を含む）を行う			2	エラー監視を行う		
C.4.1.1	開発用環境の設置有無	0	情報システムの開発用環境を設置しない						
C.4.2.1	試験用環境の設置有無	2	専用の試験用環境を設置する						
C.5.9.1	定期報告会実施頻度	3	四半期に1回						
C.5.9.2	報告内容のレベル	1	障害報告のみ						
C.6.2.1	問合せ対応窓口の設置有無	1	ベンダーの既設コールセンターを利用する						
D.1.1.1	システム移行期間	4	2年未満			1	3ヶ月未満		
D.1.1.3	並行稼働の有無	1	有り			0	無し		
E.3.1.2	Web診断実施の有無	1	実施						

調査票１．「都道府県の業務・情報システム分類に対するアンケート調査票」

●業務-システムの分類に関するアンケート調査票(案)
① 都道府県の業務-システムを平常時、災害時における分類の考え方(「【添付資料】業務-システムの分類について」をご参照ください)に沿って、AからIのシステム群での分類をお願いいたします。
② 貴県の情報システム運用状況を踏まえたシステムの分類をお願いいたします。

もしシステム毎にグループが違う場合には、
このように分けて記載ください。
違わない場合は、アルファベット一文字を記載ください。

■業務-システム一覧

No	業務	システム例	グループ	分類理由
記載例	○○○○	○○管理、■■管理 等	H ○○管理 G ■■管理	○○管理は、○○の管理に使うことを想定している。平常時はほぼ利用しない。災害対策に必要だが、直後には必要ない。 ■■管理は、■■の管理に使うことを想定している。平常時はほぼ利用しない。災害時は直後から必要。
1	税	県民税、事業税、自動車税 等		
2	電子申請・調達	電子申請、電子調達、住民向け施設予約 等		
3	財務会計	財務会計、土木積算 等		
4	学校教育	校務支援 等		
5	庶務事務	勤怠管理、旅費管理 等		
6	人事給与	人事、給与 等		
7	文書管理	公文書管理、電子決裁 等		
8	統計	人口統計 等		
9	住民向け情報提供	ホームページ、緊急通報 等		
10	内部情報共有	メール、会議室予約 等		
11	災害時対策専用	被災者支援、防災情報管理 等		
12	社会教育	図書館、博物館管理、生涯学習支援 等		

図－25　都道府県の業務・システム分類に対するアンケート調査票

調査票２．「市町村の業務・情報システム分類に対するアンケート調査票」

●業務-システムの分類に関するアンケート
① 市町村の業務-システムを平常時、災害時における分類の考え方(「【添付資料】業務-システムの分類について」をご参照ください)に沿って、AからIのシステム群での分類をお願いいたします。
② 貴市の情報システム運用状況を踏まえたシステムの分類をお願いいたします。

もしシステム毎にグループが違う場合には、
このように分けて記載ください。
違わない場合は、アルファベット一文字を記載ください。

■業務-システム一覧

No	業務	システム例	グループ	分類理由
記載例	○○○○	○○管理、■■管理　等	H ○○管理 G ■■管理	
1	住民情報	住民記録、印鑑登録、戸籍、住登外管理　等		
2	税	個人住民税、法人税、軽自動車税、固定資産税　等		
3	国保・年金	国民健康保険、国民年金　等		
4	福祉	高齢者福祉、障碍者福祉、乳幼児医療、健康管理　等		
5	選挙	選挙人名簿、期日前投票　等		
6	電子申請・調達	電子申請、電子調達、住民向け施設予約　等		
7	財務会計	財務会計、土木積算　等		
8	公営企業会計	上下水道料金　等		
9	学校教育	校務支援、学齢簿　等		
10	庶務事務	勤怠管理、旅費管理　等		
11	人事給与	人事、給与　等		
12	文書管理	公文書管理、電子決裁　等		
13	統計	人口統計　等		
14	住民向け情報提供	ホームページ、緊急通報　等		
15	内部情報共有	メール、会議室予約　等		
16	災害時対策	被災者支援、防災情報管理　等		
17	社会教育	図書館、博物館管理、生涯学習支援　等		

図－26　市町村の業務・情報システム分類に対するアンケート調査票

非機能要求グレード
（地方公共団体版）
利用ガイド

平成 26 年 3 月

財団法人　地方自治情報センター

目次

第１章　非機能要求グレード（地方公共団体版）の概要 1
　第１節　はじめに 1
　　１　情報システム調達仕様書における非機能要件の定義の困難性 1
　　２　非機能要求グレード（地方公共団体版）の考え方 2
　　３　非機能要求グレード（地方公共団体版）利用のメリット 4
　第２節　非機能要求グレード（地方公共団体版）の構成 5

第２章　非機能要求グレード（地方公共団体版）の対象 6
　第１節　利用者 6
　第２節　利用工程 7
　第３節　適用対象 8
　　１　情報システム調達仕様書における範囲 8
　　２　調達対象と非機能要件における範囲 8
　　３　クラウドに対する適用 10

第３章　非機能要求グレード（地方公共団体版）の利用方法 12
　第１節　活用シートの構成 12
　第２節　活用シートの項目 14
　第３節　利用手順 16
　第４節　準備作業と全庁的要求事項シートの作成 17
　　１　活用シートの記載内容の調整（必要に応じて実施）　【主な実施者：ICT 部門】 17
　　２　全庁的要求事項シートのレベル調整　【主な実施者：ICT 部門】 17
　　３　庁内の利用環境の整備　【主な実施者：ICT 部門】 18
　第５節　調達案件に応じたシートの検討 19
　　１　業務・情報システムグループの選択　【主な実施者：業務主管部門】 19
　　２　項目の取捨選択　【主な実施者：業務主管部門】 21
　第６節　業務主管部門要求事項シートの作成 22
　　１　業務主管部門要求事項シートのレベル調整 22
　第７節　実現方法要求事項シートの作成 24
　　１　RFI 等の実施　　【主な実施者：ICT 部門若しくは業務主管部門】 24
　　２　実現方法要求事項シートのレベル調整　【主な実施者：ICT 部門若しくは業務主管部門】 25
　第８節　検討結果の情報システム調達仕様書への反映 26
　　１　非機能要件の確定　【主な実施者：業務主管部門】 26
　　２　検討結果の情報システム調達仕様書への反映　【主な実施者：業務主管部門】 26

第４章　レベル調整時の留意点 29
　第１節　全庁的要求事項シート 29

第２節　業務主管部門要求事項シート 35
第３節　実現方法要求事項シート 47

用語集 54

参考資料　IPA の非機能要求グレードとの関係 59

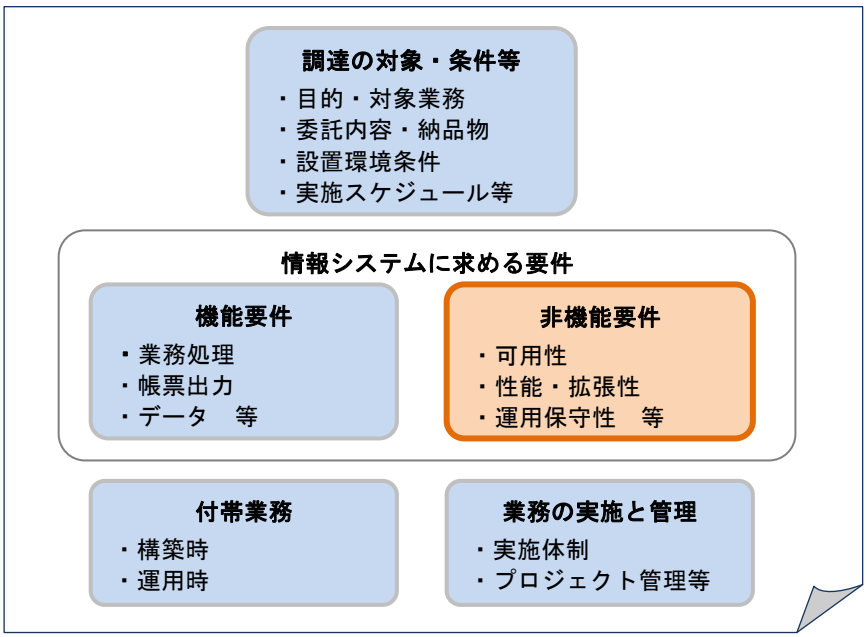
第１章 非機能要求グレード（地方公共団体版）の概要

第１節 はじめに

１　情報システム調達仕様書における非機能要件の定義の困難性

情報システムを調達するに当たっては、どのような情報システムを求めるか要件を明確にする必要があり、その内容を情報システム調達仕様書として表す必要がある。

情報システム調達仕様書に表す内容としては、大きく分けると、図－1 に示すとおり情報システムに求める要件（機能要件、非機能要件）を記載する部分の他、調達の対象や条件、付帯業務等を記載する部分がある。



図－ 1　情報システム調達仕様書の要素（項目は例）

機能要件とは、例えばどのような情報を入力し、どのような処理を行い、結果どのような出力がされるか、といった業務の実現のために情報システムが提供する機能に関する要件である。例えば、「住民の異動情報を登録・管理したい」「証明書を発行したい」といったものがそれに当たる。具体的な業務処理に関係するため、地方公共団体職員においても比較的理解しやすい。

非機能要件とは、図－1 の「情報システムに求める要件」のうち、文字どおり、この「機能要件」に関するもの以外の要件を指す。例えば、以下のような情報システムの構成や機器の数量等の根拠になるなど情報システムのコスト等に直結するものであり、情報システムを適切に調達するために、機能要件と同等以上に重要な要件である。

○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）

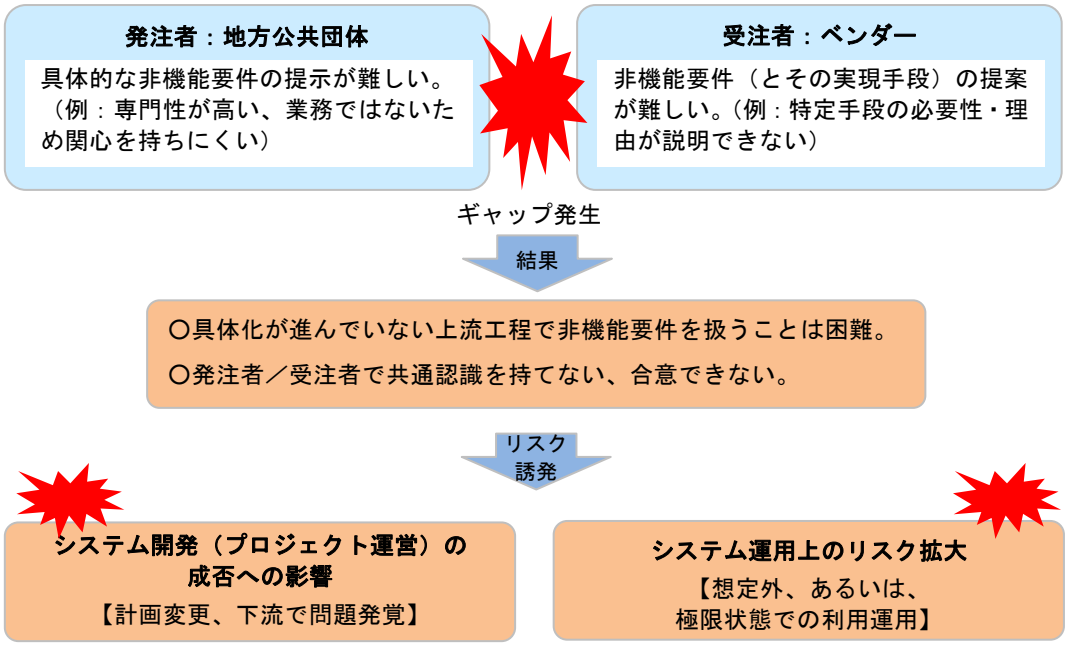
・運用スケジュール（稼働時・停止予定など）

・障害・災害時における稼働目標

○性能・拡張性（情報システムの性能及び将来のシステム拡張に関する要求）
・業務量及び今後の増加の見積り
・情報システム化対象業務の特性（ピーク時、通常時、縮退時など）
○運用・保守性（情報システムの運用と保守サービスに関する要求）
・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　等

しかし、非機能要件は、「地方公共団体の情報システム調達仕様書における非機能要件に関する調査研究報告書」（以下「調査研究報告書」という。）に示したように、地方公共団体の情報システム調達において十分に認識されていない。加えて、業務との関係が見えにくい抽象的なものが多く、技術的な内容を含むものが多いことから、機能要件に比べてどのような項目を定めるべきなのか、どの程度の要件にすべきかを決めることが難しい状況となっている。一方、ベンダー側においても、非機能要件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しにくい状況となっている。

この結果、発注者側である地方公共団体と受注者側であるベンダー間でギャップが生じ、開発や運用段階になって、トラブルが発生する大きな要因となるおそれがある（図－2）。情報システムの適切な開発、安定的な運用を図るためには、そのギャップを解消し、適切に非機能要件を定義することが重要である。



出所：IPA「非機能要求グレード利用ガイド［解説編］」,2010 年 4 月,p.4 を基に作成

図－ 2　非機能要件の定義の困難性とそれにより生じる問題点

2　非機能要求グレード（地方公共団体版）の考え方

先に示した課題を解決し、非機能要件を定義する際に有益なツールとして、独立行

政法人情報処理推進機構（以下「IPA」という。）が作成した非機能要求グレードがある。これは、発注者側である地方公共団体と受注者側であるベンダー間のギャップという問題を解消し、共通認識の形成と合意を図ることを容易にするために、以下のような基本的な考えに基づいたツールとなっている。

- 地方公共団体／ベンダー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合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、発注者が非機能要件を速やかに提示できるようにする。
- 非機能要件の実現レベルを列挙することで、ベンダーが非機能要件の実現手段を具体的に提示できるようにする。

非機能要求グレード（地方公共団体版）は、このような考え方を持つ IPA の非機能要求グレード（2013 年 4 月）を基に、地方公共団体の実情や課題を踏まえて変更した非機能要件の定義を支援するツールである。

地方公共団体の非機能要件に関する課題としては、調査研究報告書に示したとおり、表－1 に示す 5 点が挙げられる。非機能要求グレード（地方公共団体版）は、これらの課題に対応することを念頭に作成したものである。

なお、このような背景により作成したものであるため、その利用に当たっては、適時に RFI（情報提供依頼）やヒアリング等を行い、地方公共団体とベンダー間で共通認識を持つとともに合意形成を図り、双方のギャップを解消するよう利用することが肝要である。

表－1　地方公共団体における非機能要件に関する課題と非機能要求グレード（地方公共団体版）作成ポイント

項目	実態	ポイント
（1） 非機能要件という概念の浸透	・「非機能要件」という言葉については、庁内ではほぼ認識されていない。 ・情報システム調達仕様書について、機能要件に比べて非機能要件は記載が少ない。	・用語を含め、地方公共団体の業務主管部門職員にとっても分かりやすくする。
（2） 適切な非機能要件の定義ができる手法の確立	・業務主管部門が実施することが多い。 ・その際、ICT 部門が支援していることが多い。	・このような地方公共団体で一般的な情報システム調達仕様書の作成手順を踏まえる。
（3） 発注者と受注者の合意と非機能要件の標準化	・ベンダーに対して RFI やヒアリングの実施等、合意形成が重要である。	・ベンダーに確認する手順を組み込む。
（4） 地方公共団体の特性を考慮した非機能要件の標準化	・民間企業等との情報システムの特性に違いがある。 ・民間企業等との調達・契約行為の性格に違いがある。	・これらの民間企業等との違いを踏まえる。
（5） 情報システムの調達における職員負担の軽減	・特に人的余裕のない中小規模の地方公共団体では情報システム調達仕様書の作成は負担になる。	・検討項目を精査し、資料のボリュームも削減する。

３　非機能要求グレード（地方公共団体版）利用のメリット

非機能要求グレード（地方公共団体版）を利用して情報システムの調達を行うことのメリットとして、図－3 に示すような点が挙げられる。非機能要求グレード（地方公共団体版）は、このようなメリットを持つものであり、地方公共団体の非機能要件の適切な定義の一助となり、情報システムの適切な開発、安定的な運用に資することを目指したものである。

〇調達に当たって重要な非機能要件を網羅的に定義できる。
〇具体的な項目と選択肢が示され、発注者と受注者の共通認識の形成がしやすい。
〇地方公共団体の業務・情報システムの特性に合わせた推奨される要件の指標が予め示されており、効率的に検討作業ができる。

図－ 3　非機能要求グレード（地方公共団体版）利用のメリット

第２節 非機能要求グレード（地方公共団体版）の構成

非機能要求グレード（地方公共団体版）の構成は、表－2 に示すとおりである。IPA の非機能要求グレードと非機能要求グレード（地方公共団体版）の成果物との対応関係と主な変更の内容は、巻末の参考資料を参照されたい。

表－ 2　非機能要求グレード（地方公共団体版）の成果物と使い方

成果物	概要と使い方
調査研究報告書	調査研究内容をまとめたもの。 非機能要求グレード（地方公共団体版）の背景や考え方の理解のために参照する。
利用ガイド （本書）	非機能要求グレード（地方公共団体版）の利用方法を示したもの。 非機能要求グレード（地方公共団体版）を利用して情報システム調達仕様書を作成する際に参照する。
項目一覧	非機能要件項目の体系を示したもの。 非機能要件の全体像を理解するときに利用する。 また、各地方公共団体において加工することにより、チェックシートや RFI の回答シート等に利用することができる。
活用シート	非機能要件を検討するためのツール（エクセルシート）。 具体的に情報システム調達仕様書における非機能要件の検討作業のために利用する。

第２章 非機能要求グレード（地方公共団体版）の対象

ここでは、非機能要求グレード（地方公共団体版）が想定している対象について示す。なお、その考え方や理由の詳細については、調査研究報告書を参照されたい。

第１節 利用者

非機能要求グレード（地方公共団体版）では、主な利用者として、情報システム調達仕様書を作成する地方公共団体職員を想定している。

情報システム調達仕様書の作成の担い手は地方公共団体によって異なるが、非機能要求グレード（地方公共団体版）では、表－3 に示すような分担により情報システム調達仕様書の作成がされることを想定している。

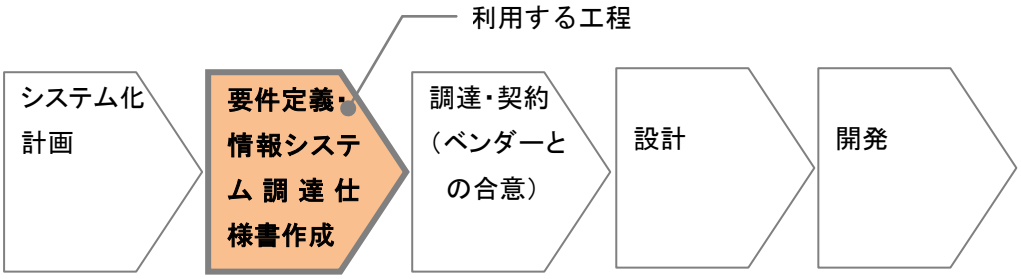
表－ 3　情報システム調達仕様書の作成に関する主体

主体	役割
業務主管部門職員　（＊）	業務を主管する立場から、情報システムに必要な要件を検討し、情報システム調達仕様書として取りまとめる。
ICT 部門職員	全庁的な ICT 規定に関する事項や技術的な知識を特に必要とする事項に関して要件の検討を行い、情報システム調達仕様書として取りまとめる。若しくは、業務主管部門の検討を支援する。
ベンダー	情報システム調達仕様書の作成に必要な事項について、開発・運用する立場から情報提供等を行う（情報提供依頼への対応）。

（＊）全庁的な基盤システム等、ICT 部門が主体的に情報システム調達仕様書を作成すべき情報システムについては、ICT 部門がその業務を主管する部門と読み替える。

第２節 利用工程

非機能要求グレード（地方公共団体版）では、情報システムの構築に向けてのプロセスのうち、図－4 に示すように、要件定義・情報システム調達仕様書作成の工程で利用することを想定している。



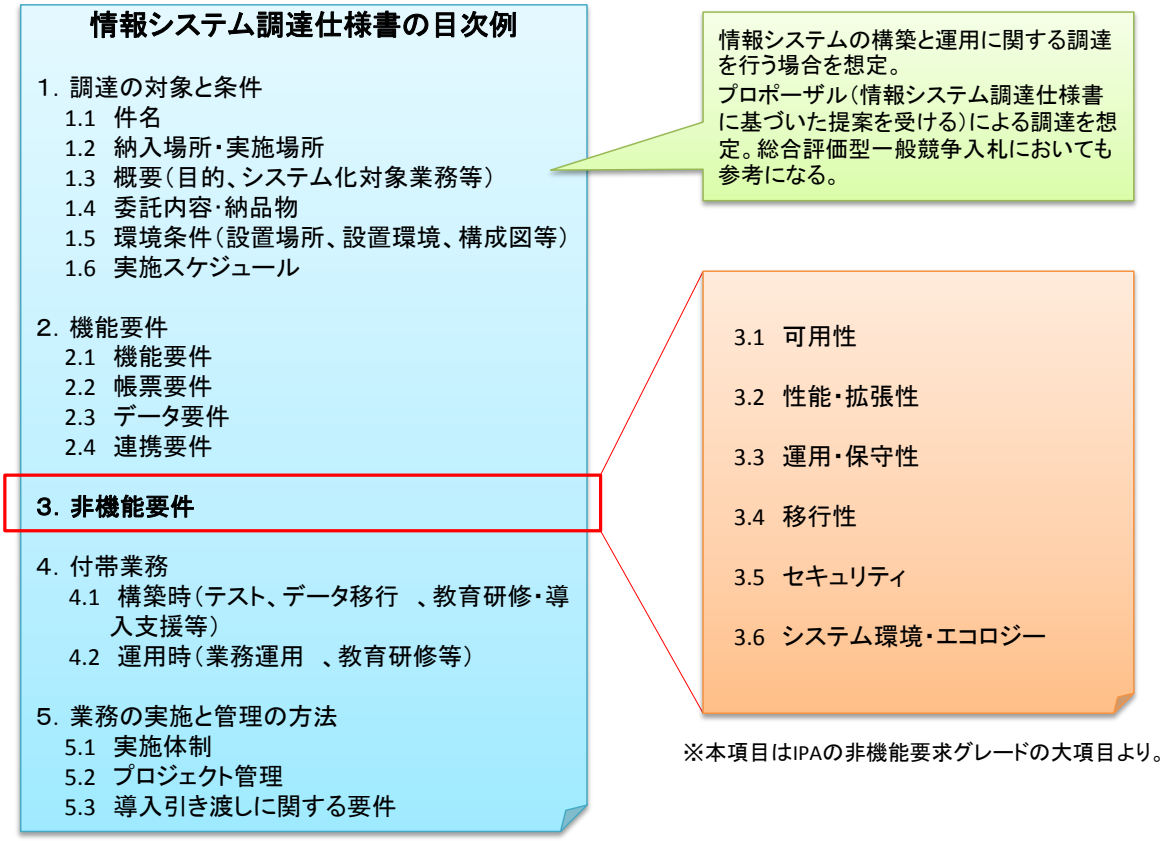
図－ 4　非機能要求グレード（地方公共団体版）で利用する工程

第３節 適用対象

１　情報システム調達仕様書における範囲

先述のように、非機能要求グレード（地方公共団体版）は、情報システム調達仕様書の作成を利用対象としている。情報システム調達仕様書の目次例を図－5 に示す。

非機能要求グレード（地方公共団体版）は、このうち、先述のように非機能要件に当たる部分を作成するためのツールである。



図－ 5　非機能要求グレード（地方公共団体版）の情報システム調達仕様書の中での取扱範囲

２　調達対象と非機能要件における範囲

非機能要求グレード（地方公共団体版）では、情報システムの構築と運用の調達において利用することを想定している。

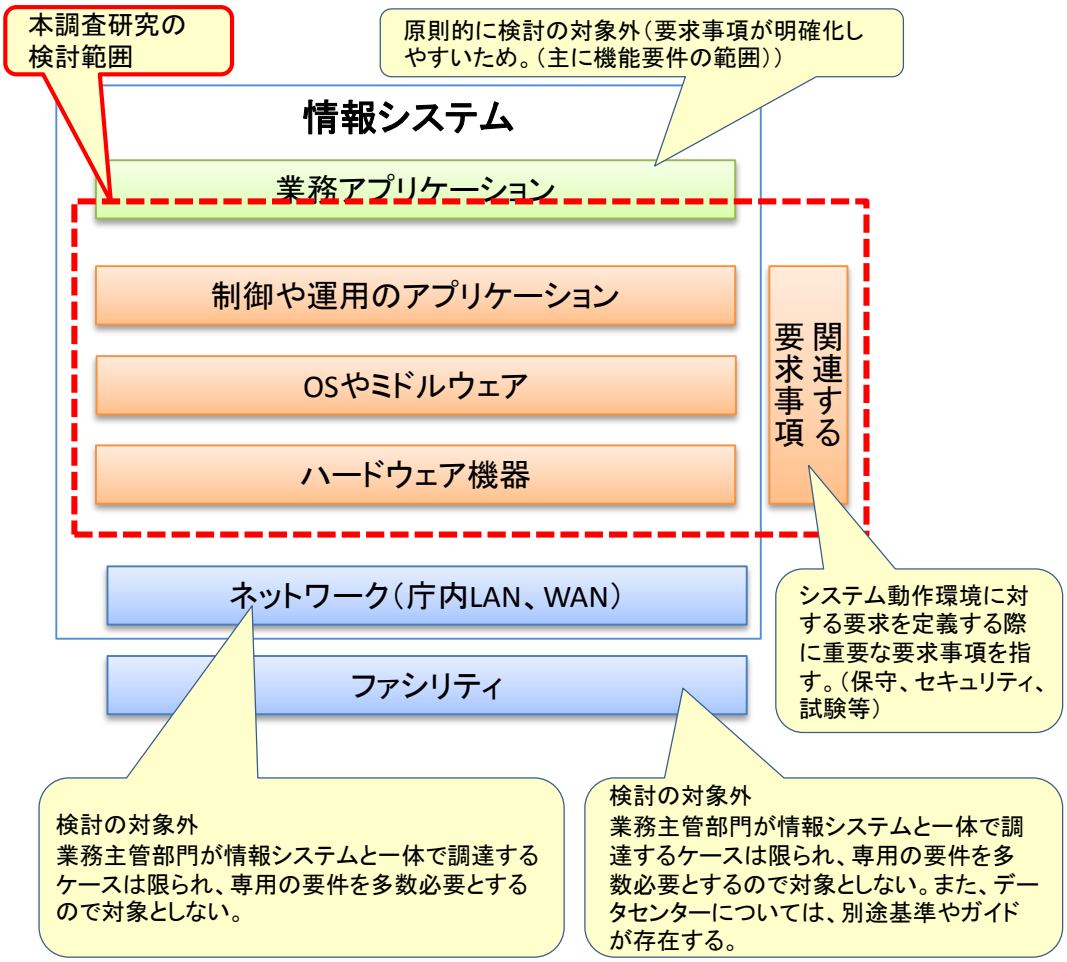
---

[1]データ移行は、情報システムを新規に構築するより再構築をする場面が増える中で、仕様として示す内容として特に重要である。非機能要件グレード（地方公共団体版）でも基本的な移行性の要件は含まれているが、より詳細にデータの権利の帰属（基本的に各団体に帰属する）、対象データ項目・形式、関係者の役割分担等を示す必要がある。データ形式については、中間標準レイアウト仕様の対象業務となっている情報システムについては、中間標準レイアウト仕様を指定することが望ましい。中間標準レイアウトとは、情報システムの変更に伴うデータ移行時に使用する中間ファイルのデータ項目やその表現形式等を標準化したレイアウト仕様のことである。これを利用することにより、データ移行作業が明確化されるため、従来不明瞭であったデータ移行作業量も透明化され、データ移行にかかるコストの削減が期待できる。
総務省「中間標準レイアウト仕様」＜http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/02kiban07_03000024.html＞（最終アクセス平成 26 年 2 月 5 日）。

[2]ここでは、情報システム固有に必要なバッチジョブ管理、印刷、データパンチ等を指す。

対象とする情報システムは、各業務主管部門で調達する個別システムを主眼に置いている。このため、全庁的に調達されることが多いファシリティやネットワーク等については、原則的に非機能要求グレード（地方公共団体版）の対象としていない。これらが含まれる調達においては、別途、これらの項目も含めて検討する必要がある。また、ネットワークを通じて他の情報システムと連携しているような場合には、対象システムだけでなく、関係するシステム全体を含む要件を検討する必要がある。今後、社会保障・税番号制度に対応した情報システムの構築・運用に当たっては、外部システムとの連携が重要になると考えられる。その際には、当該システムだけでなく、情報システム全体として要件を満たしているのかのチェックも、非機能要求グレード（地方公共団体版）を利用しての要件の検討とは別に留意する必要がある。

また、非機能要件は、主に情報システム環境（ハードウェア機器、OS やミドルウェア等のソフト、制御や運用を行うソフトウェア）により実現されるため、これらの情報システム環境を対象の主眼としている（図－6）。



出所：IPA「非機能要求グレード利用ガイド（解説編）」,2010 年 4 月,p.2 を基に作成

図－ 6　対象となる非機能要件の範囲

対象外とした事項で、非機能要件として考慮する必要があるものをまとめると、具体的に表－4 に示すような事項がある。これらの事項のうち、調達対象に含める必要

のある事項は、別途検討を行い、非機能要件に加える必要がある。また、既存のファシリティやネットワーク等を利用する場合には、情報システム調達仕様書に前提条件として記すことを検討する（図－5 の「1.5　環境条件（設置場所、設置環境、構成図等)」に相当する箇所に記載する)。また、それらの前提条件を利用して、調達対象となる情報システムが支障なく動作することや利用可能であることを、要件として示す必要がある。

表－ 4　非機能要件グレード（地方公共団体版）で対象外とした要件項目例

分類	要件項目例	概要	IPA 非機能要求グレードの項目
ネットワーク（ネットワークセキュリティ対策含む）	回線の冗長化	ネットワークを構成する伝送路を物理的に複数用意し、耐障害性を高める度合いに関する項目。	A.2.4.1
	通信制御	不正な通信を遮断するための制御を実施（ファイアーウォール等の導入）するかを確認するための項目。	E.8.1.1
	不正通信の検知範囲	ネットワーク上において、IDS 等を導入することにより、不正追跡・監視を実施し、情報システム内の不正行為や、不正通信を検知する範囲を確認するための項目。	E.8.2.1
	ネットワーク攻撃への対策	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。	E.8.3.1
ファシリティ	耐震震度	情報システムを設置する施設の耐震震度に関する項目。	F.4.1.1
	床耐荷重	情報システムを設置する施設の床の耐荷重に関する項目。	F.4.3.1
	停電対策	情報システムを設置する場所の停電時の対策実施に関する項目。	F.4.4.4
	不正監視対象（侵入者・不正操作等）	不正な侵入者等を監視するために設置する監視カメラ等による監視の範囲に関する項目。	E.7.1.5

※上記の項目で調達対象とするものがある場合には別途検討し要件に含める。既存のものを利用する場合には、その旨を前提条件として情報システム調達仕様書に示す。

3　クラウドに対する適用

非機能要求グレード（地方公共団体版）では、ハードウェアやソフトウェアを自己導入する形態を主眼としている。

しかし、非機能要求グレード（地方公共団体版）で検討した内容を、クラウド利用時における要件項目や SLA（Service Level Agreement）の項目の検討に利用することは可能である。ただし、活用シートには、クラウド利用時に適用する場合には、必要としない項目があるため、「クラウド調達時の扱い」という欄を設け、クラウド利用時に必要な項目か不要な項目かを区別できるようにしている。「第３章第５節　２項目の取捨選択」を参照の上、項目の吟味を行う。さらに、後述する選択レベルを検

討する際には、クラウド利用時の留意事項を「第４章　レベル調整時の留意点」や活用シートの備考等に記載しているので、それらを参考に検討する。

なお、クラウド調達の際には、サービスの選定や ASP･SaaS 事業者との契約、サービス導入後の運用などの考え方を解説する総務省「地方公共団体における ASP・SaaS 導入活用ガイドライン」[3]を参照することが有益である。

[3] 総務省「『地方公共団体における ASP･SaaS 導入活用ガイドライン』の公表及び意見募集の結果」＜http://www.soumu.go.jp/menu_news/s-news/02gyosei07_000026.html＞（最終アクセス平成 26 年 2 月 5 日）。

第３章 非機能要求グレード（地方公共団体版）の利用方法

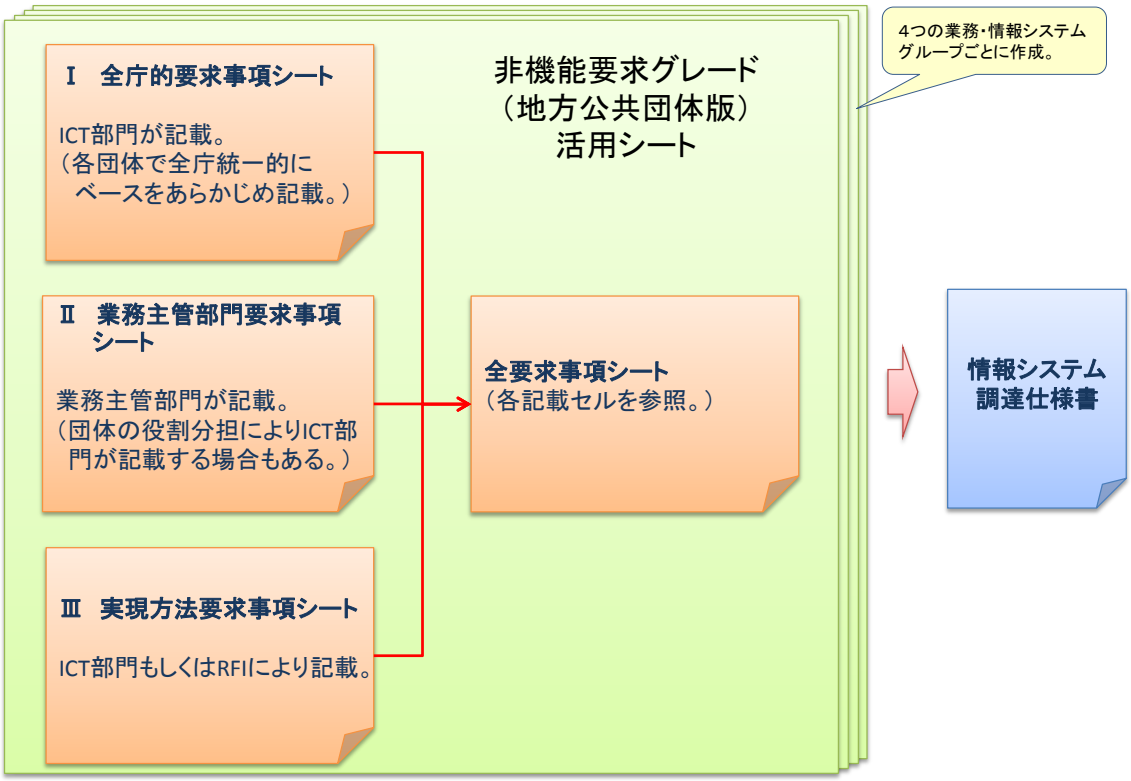
第１節 活用シートの構成

非機能要件を検討するに当たっては、非機能要件の項目とそれぞれの要件のレベルを設定し、具体化していくための「活用シート」を利用する。

活用シートは、図－7 に示すように、「全庁的要求事項シート」「業務主管部門要求事項シート」「実現方法要求事項シート」「全要求事項シート」の 4 種類から構成される。この 4 種類のシートのセットは、後述するように、業務・情報システムの重要度等に応じた 4 つのグループごとに用意されている。

「全庁的要求事項シート」は、全庁的な環境条件や共通的な規定により定められる要求事項をシート化したものであり、ICT 部門が内容を検討することを想定している。「業務主管部門要求事項シート」は、業務主管部門において、業務利用する立場から明確化できる基本的な要求事項をシート化したものである。「実現方法要求事項シート」は、業務主管部門要求事項や全庁的要求事項を踏まえ、情報システム調達仕様書に示すべき情報システムによる実現方法に関する要求事項をシート化したものである。ベンダーに対する RFI（情報提供依頼）等に基づき業務主管部門が検討するか、あるいは ICT 部門が内容を検討することを想定している。「全要求事項シート」は、「全庁的要求事項シート」「業務主管部門要求事項シート」「実現方法要求事項シート」で規定した内容を集約し、情報システム調達仕様書作成を支援するためのシートである。

情報システム調達仕様書の作成に際しては、この 4 種類のシートを利用して非機能要件を検討する



図－ 7 4 つの活用シートの構成

なお、RFI とは、情報システムの調達に当たり、発注先候補となるベンダーに対して、要件等を決定するために必要な技術情報や製品情報、見積り等の情報の提供を依頼すること、あるいはその文書を指す。

予算の範囲内で合理的な要件を定義し、適切に調達・契約するためには、一方的な情報システム調達仕様書とならないよう、ベンダーからの意見を広く聴取して、確認をしていくことが重要である。特に実現方法要求事項シートについては RFI の実施を想定しているが、実現方法要求事項シートに限らず、他のシートでの検討事項についても、RFI やヒアリングの場面を作り、ベンダーに対して確認を行いながら要件の検討を行っていくことが重要である。

RFI の実施方法の概略については、「第 7 節　1　RFI 等の実施」に示す。

第２節 活用シートの項目

活用シートの各欄の内容は、表－5 に示すとおりである。

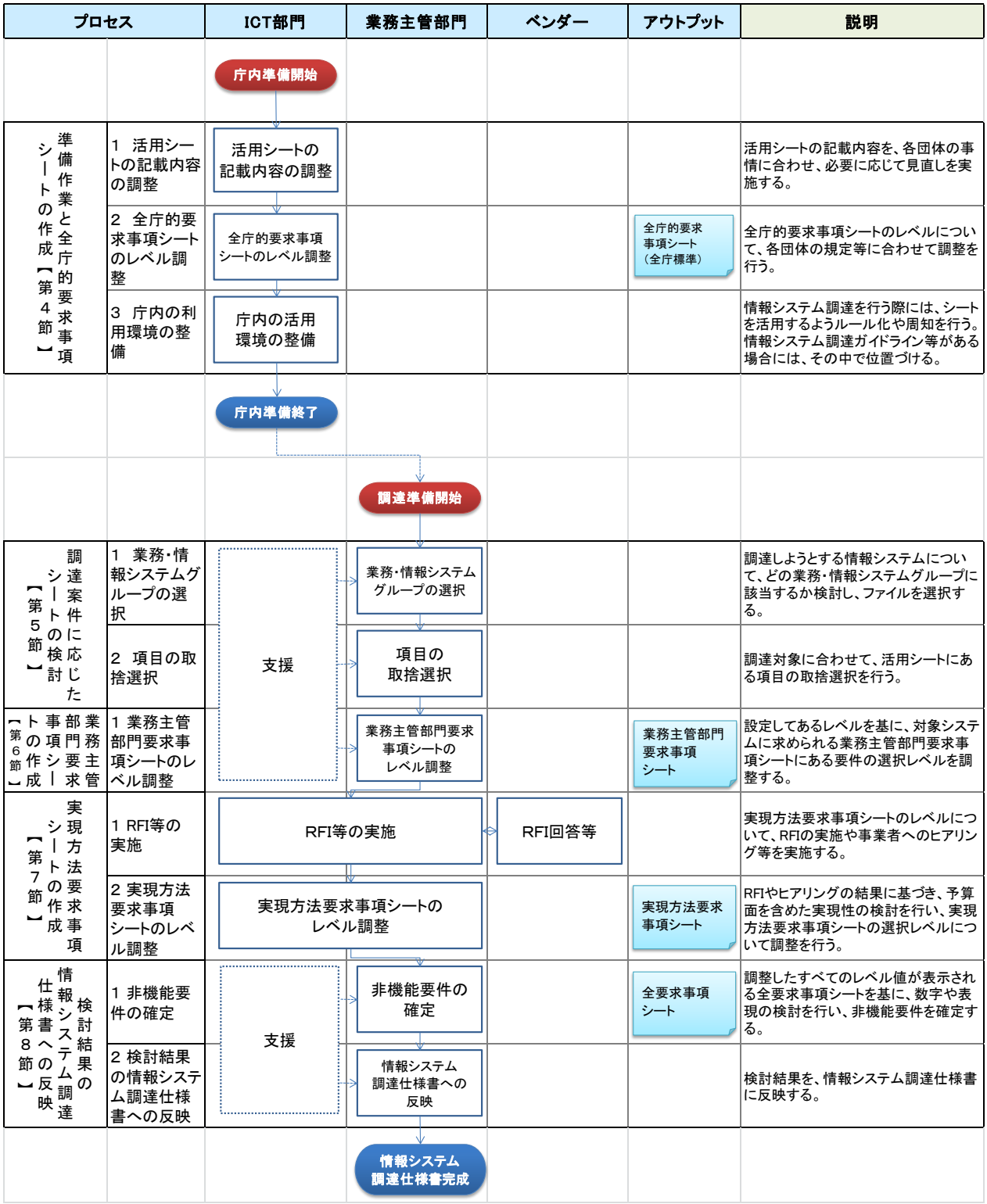
表－ 5　活用シートの各項目の説明

項目	内容
項番	活用シートの項目（メトリクス）を識別するための連番。 IPA の非機能要求グレードに対応する項目は、その項番を引き継いでいる。地方公共団体版で追加した項目は、新たな項番を付与している。
大項目	非機能要件を体系的に整理したときの最も広い分類。
中項目	非機能要件を体系的に整理したときの大項目を細分化した分類。
メトリクス（指標）	中項目を細分化した、要件項目を定量的に表現するための指標。 情報システム調達仕様書は、このメトリクスの単位で検討する。
メトリクス説明	メトリクスの内容や考え方を示す説明。
選択レベル	当該業務・情報システムのグループにおいて、実現性（コスト面）も加味しながら、標準的と思われるレベルを選択したもの。
選択時の条件	選択レベルの値の条件を補足説明したもの。 また、「＋」「－」は、要件を検討する際に、選択レベルを基にレベルを上げる、下げる場合の条件を示している。
クラウド調達時の扱い	クラウドによる情報システム調達の場合に、当該項目が要件として示すことがふさわしい項目かどうかを分類して示したもの。クラウドの場合、例えば、ハードウェアについては、ベンダー側が自らの創意工夫で用意するものであり、ハードウェアに関する要件を厳密に指定することは適さない。このような項目は適さないものとして分類し、示している。 【凡例】 〇：クラウドの対象と成り得る項目 △：クラウドの対象となる場合がある項目 －：クラウドの対象とはならない項目
検収時の扱い	情報システムを調達した際に、当該項目について、検収時にどのように扱うべきかを示したもの。非機能要件においては、例えば、稼働率やレスポンスタイムのように、当該要件を満たしていることを厳格に判定する項目や、厳格に満たそうとした場合にはコストが増加する可能性がある項目がある。このような項目については、満たすことが「必須」の要件として示すのではなく、「目標」として示すべき項目として分類している。 このような「目標」として示す要件は、サービスレベルマネジメント（SLM）の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。 SLM では、サービスの提供者と利用者の間でサービスの仕様のほか、品質や成果に関する評価基準や測定方法を定める。提供者は、定めた事項に基づき測定を行い、定期的にサービスの品質や成果を利用者に報告する。両者は報告に基づいて問題点と解決方法を検討する。 【凡例】 〇：目標（値）として扱い、長期的に測定・評価を行うべき項目
利用ガイドの解説	「利用ガイド」第 4 章においてレベル調整時の留意点について解説しているので、その掲載ページを示している。

項目	内容
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 の最大 6 段階に整理した項目。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示す。 また、「－」は仕様の対象外とする場合、「＊」はベンダーの提案事項とする場合の選択肢である。 開発コストとは、要件定義後から情報システムが出来上がって稼働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、情報システムの設計、導入時作業など情報システムの環境に関わるすべてのコストが含まれる。 また、レベル値はメトリクスごとに独立して設定している。同じレベル値は、同じ難易度を示すものではない。
備考	メトリクスごとの補足説明。項目一覧の構成で表現しきれない点を補足している。 備考列の内容が、活用シートのどの列に対応するものかを明記するため、以下のように表示している。 ・【メトリクス】、【レベル】などのような列名は【　】で囲んで表示する。 ・特定レベルへのコメントの場合は【レベル 0】のような表示とする。 ・メトリクス全般の注意事項は【注意事項】と表示する。

第３節　利用手順

非機能能要求グレード（地方公共団体版）の利用方法の基本的な手順は図－8 のとおりである。



図－ 8　非機能要求グレードを利用した情報システム調達仕様書の策定手順

第４節 準備作業と全庁的要求事項シートの作成

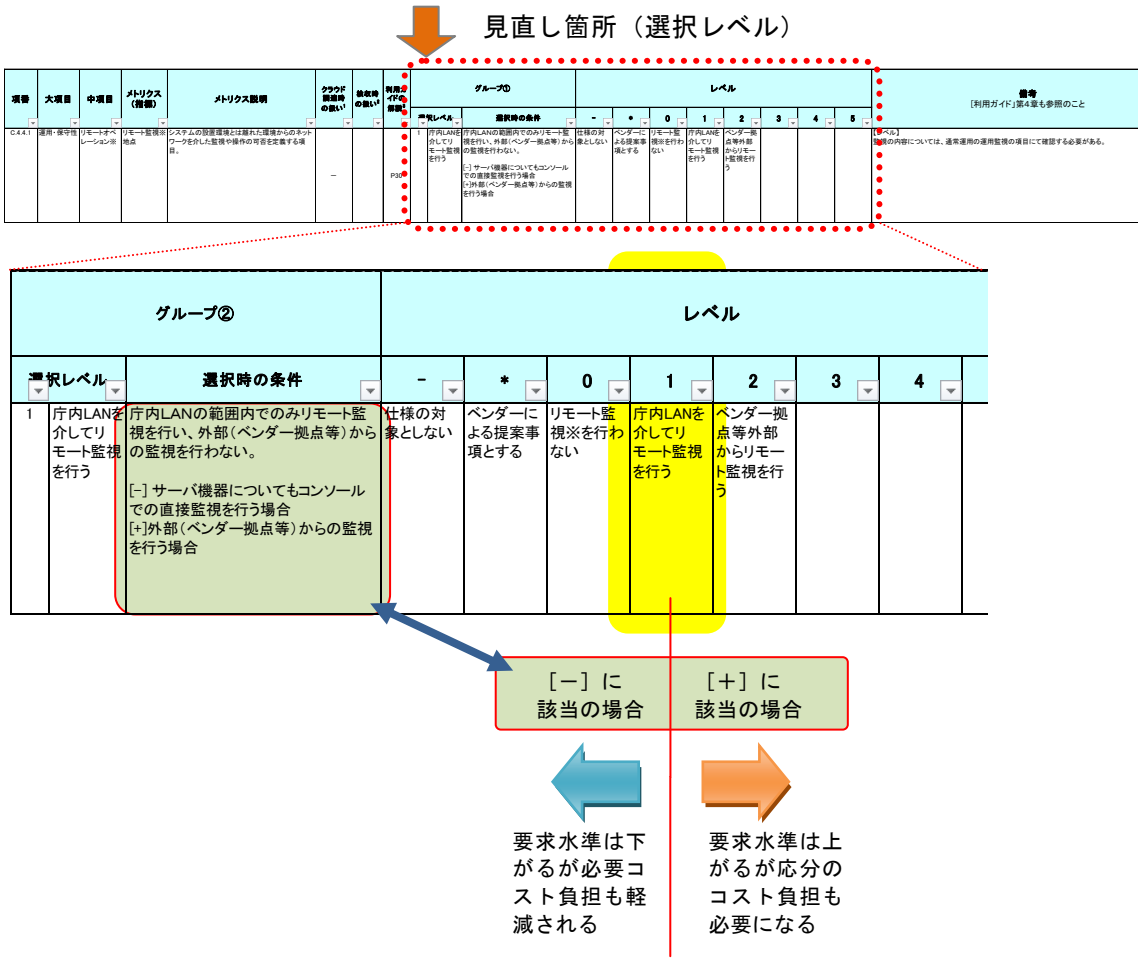
活用シートは、地方公共団体で利用できるように作成してあるが、各地方公共団体の実状に応じた見直しを行うとともに、その利用を促すための取組を実施する。

１　活用シートの記載内容の調整（必要に応じて実施）　【主な実施者：ICT 部門】

活用シートは、地方公共団体がなるべく理解しやすいよう用語表現の調整を実施している。しかし、もし各地方公共団体の事情により、言い換えをした方がよい場合は、必要に応じて庁内で理解しやすいよう、記載内容や表現の見直しを行う。ただし、その場合には、シート全体の整合が取れているか（表現や用語を変えたことにより、矛盾や齟齬が生じていないか）、対外的に意図が正確に伝わるかという観点からも留意が必要である。

２　全庁的要求事項シートのレベル調整　【主な実施者：ICT 部門】

活用シートのうち「全庁的要求事項シート」は、一般的に情報システム個別に定めるのではなく、全庁的な規定や情報システムの環境等に基づき、選択レベルを設定すべき事項である。活用シートでは、一般的に地方公共団体で設定されていると思われる値で設定してあるが、各地方公共団体において必要に応じて見直す。



図－ 9　全庁的要求事項シート見直し箇所

具体的には、以下のような各地方公共団体が定めた関連規定等に基づき、4 つの業務・情報システムグループそれぞれの全庁的要求事項シートのレベルの調整を行う。調整に当たっては、各活用シートの「選択時の条件」欄に記載された事項を考慮する。文頭に［＋］（プラス）と書かれた事項に該当する場合はレベルを上げることを検討する必要がある。反対に［－］（マイナス）と書かれた事項に該当する場合はレベルを下げることを検討する（図－9）。

・情報セキュリティポリシー
・情報システム調達ガイドライン
・全庁的に利用する情報システム機能に関する設計書
・環境配慮のための規定　等

レベル調整に当たって、特に留意すべき項目については、各シートに記載しているほか、「第４章　レベル調整時の留意点」に示しているので、参照の上、検討する。

３　庁内の利用環境の整備　【主な実施者：ICT 部門】

準備が完了した活用シートについて、庁内での利用を推進するために、標準的な手順として位置づけるとともに周知を図る。

例えば、以下のような取組を実施する。

・活用シートの利用のルール化と庁内周知を行う。
・情報システム調達ガイドライン等を策定している地方公共団体であれば、当該ガイドライン等において、情報システム調達仕様書作成の際に本活用シートを利用する旨を示す。
・情報システム調達仕様書作成に当たっての標準様式として、本活用シートを庁内に周知、提供する。

第５節 調達案件に応じたシートの検討

調達対象となる情報システムに合わせて、適切な活用シートを選択するとともに、必要な項目の取捨選択を行う。

１　業務・情報システムグループの選択　【主な実施者：業務主管部門】

非機能要求グレード（地方公共団体版）では、業務・情報システムの重要度等に応じて 4 つのグループを設定している。非機能要件を検討するに当たり、調達対象システムがどのグループに属するかを検討する。

活用シートは、この 4 つのグループのものが用意されている。各シートでは、それぞれの業務･情報システムのグループに分類される情報システムを想定したときに標準的と思われる選択レベルが設定してある。

4 つの種類の分類の基準は図－10 に示すとおりである。なお、このように 4 つに分類した検討経緯の詳細は、調査研究報告書を参照されたい。

○平常時の分類基準

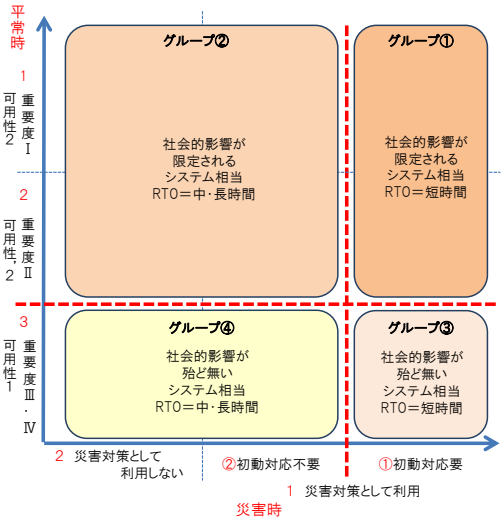
分類	「可用性」による分類		重要性分類	
	分類	分類基準	分類	分類基準
1	可用性2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害されるおそれがある情報資産	Ⅰ	個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
2	可用性2’	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	Ⅱ	公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
3	可用性1	可用性2の情報資産以外の情報資産	Ⅲ	外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
			Ⅳ	上記以外の情報。

出所：総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」を基に作成

○災害時の分類基準

分類		細目		分類基準
1 災害対策として利用	① 初動対応要	目標開始時間	1時間以内	応急業務のうち、発災後、直後の対応が求められる業務
			3時間以内	応急業務のうち、発災後、速やかに対応すべき業務
			6時間以内	平常時の業務に戻すために初動で必要になる対応業務
	② 初動対応不要			初動対応は不要だが、災害対策として利用される業務
2 災害対策として利用しない		－		災害対策としては利用が想定されない業務

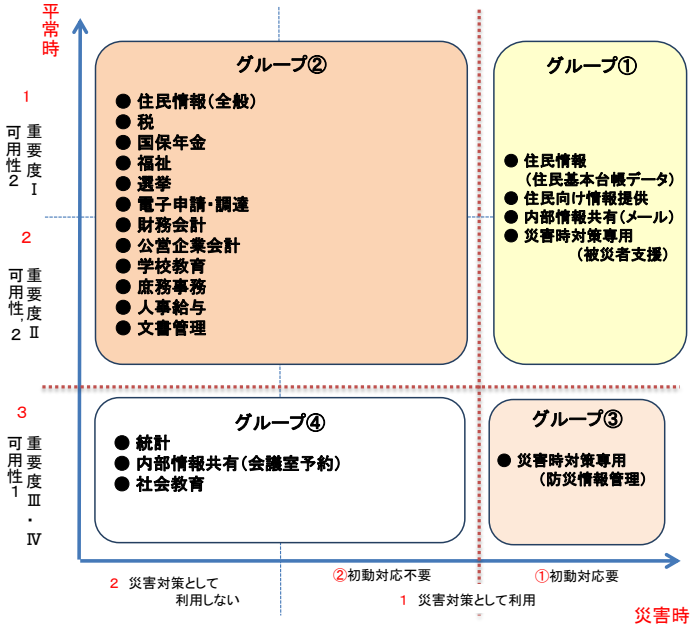
出所：総務省「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」、「ICT部門の業務継続計画＜初動版解説書＞



図－ 10　業務・情報システムの分類の基準

一般的な地方公共団体の業務・情報システムについて、この基準を基にプロットした例を図－11 に示す。上記の基準と業務・情報システムの分類例から、調達対象システムについて最も近いと考えられる分類の活用シートを選択する。なお、この分類例は、あくまで例示であり、各地方公共団体の考え方によっても変わるものと考える。必ずしも例示どおりに活用シートを選択する必要はなく、各地方公共団体の基準に照らし合わせながら適切なものを選択する。

なお、判断に迷った場合には、地方公共団体の情報システムで最も多くの種類の業務･情報システムが該当すると考えられる分類②の活用シートを利用することも一案である。



都道府県のシステム

No	業務	情報システム例	グループ
1	税	県民税、自動車税、固定資産税　等	②
2	電子申請・調達	電子申請、電子調達、住民向け施設予約　等	②
3	財務会計	財務会計　等	②
4	上下水道	上下水道　等	②
5	学校教育	校務支援　等	②
6	土木積算	土木積算　等	②
7	庶務事務	勤怠管理、旅費管理　等	②
8	人事給与	人事給与　等	②
9	文書管理	公文書管理　等	②
10	統計	人口統計　等	④
11	住民向け情報提供	ホームページ、緊急通報等	①
12	内部情報共有(メール)	メール　等	①
13	内部情報共有（会議室予約）	庁内会議室予約　等	④
14	災害時対策専用（被災者支援）	被災者支援、職員安否確認等	①
15	災害時対策専用（防災情報管理）	災害情報収集、防災対策情報共有　等	③
16	社会教育	図書管理、web 予約、蔵書検索　等	④

市町村のシステム

No	業務	システム例	グループ
1	住民情報（全般）	住民記録、印鑑登録、戸籍　等	②
2	住民情報(住民基本台帳データ)	住民基本台帳データ参照・出力　等	①
3	税	市町村税、法人税、軽自動車税　等	②
4	国保・年金	国民健康保険、国民年金　等	②
5	福祉	高齢者福祉、乳幼児医療　等	②
6	選挙	選挙人名簿、期日前投票　等	②
7	電子申請・調達	電子申請、電子調達、住民向け施設予約　等	②
8	財務会計	財務会計、上下水道会計　等	②
9	土木積算	土木積算　等	②
10	上下水道	上下水道　等	②
11	学校教育	校務支援、学齢簿　等	②
12	庶務事務	勤怠管理、旅費管理　等	②
13	人事給与	人事給与　等	②
14	文書管理	公文書管理	②
15	統計	人口統計　等	④
16	住民向け情報提供	ホームページ、緊急通報　等	①
17	内部情報共有(メール)	メール　等	①
18	内部情報共有（会議室予約）	庁内会議室予約　等	④
19	災害時対策専用（被災者支援）	被災者支援、職員安否確認等	①
20	災害時対策専用（防災情報管理）	災害情報収集、防災対策情報共有　等	③
21	社会教育	図書管理、web 予約、蔵書検索　等	④

図－ 11　業務・情報システムの分類例

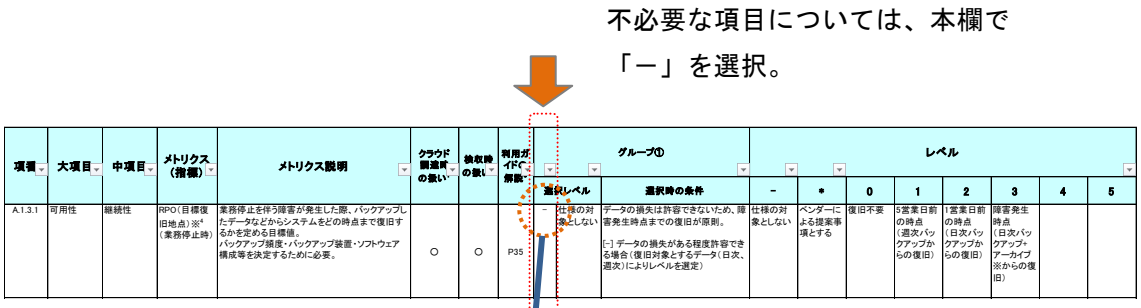
２　項目の取捨選択　【主な実施者：業務主管部門】

活用シートでは、情報システムを調達するに際して定めることが望ましい非機能要件項目を、幅広く収めている。各地方公共団体や調達する情報システムの状況に応じて項目の取捨選択を行う。特に調達する案件の形態や性格によっては、定める必要がない項目がある可能性があり、非機能要件を検討するに当たってはそれぞれの項目の必要性について吟味する必要がある。例えば、以下のような例の場合には、不必要な項目がある。

- クラウドにより導入する情報システムの場合（ベンダー側の創意工夫で用意するハードウェア等については、要件として示すことはそぐわない）
- 新規システムの調達の場合（移行に関する項目は不要）
- 調達対象でない要件（例：既存の情報システムや機器で実現するもので、要件として特に明示の必要がないもの）

このうち、クラウドを適用した情報システムの場合の項目の適用については、「クラウド調達時の扱い」欄に適否を示しているので参考に検討する。

必要のない項目がある場合には、その項目の「選択レベル」欄について数字ではなく「－」（ハイフン）を選択する。「－」を選択すると、最終的に情報システム調達仕様書の基となる「全要求事項シート」において、情報システム調達仕様書記載例に不必要な項目であることが判別できるように表示される。「－」を選択した事項は、最終的な情報システム調達仕様書から削除する必要がある。（図－12）。



項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い	検収時の扱い	利用ガイド解説	グループ①		レベル							
								選択レベル	選択時の条件	－	*	0	1	2	3	4	5
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	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。バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	－	データの損失は許容できないため、障害発生時点までの復旧が原則。 [-] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	仕様の対象としない	ベンダーによる提案事項とする	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）		

全要求事項シートでの表現の例

情報システム仕様書記載例		
○○については、	仕様の対象としない	。

図－ 12　不必要な項目についての設定方法

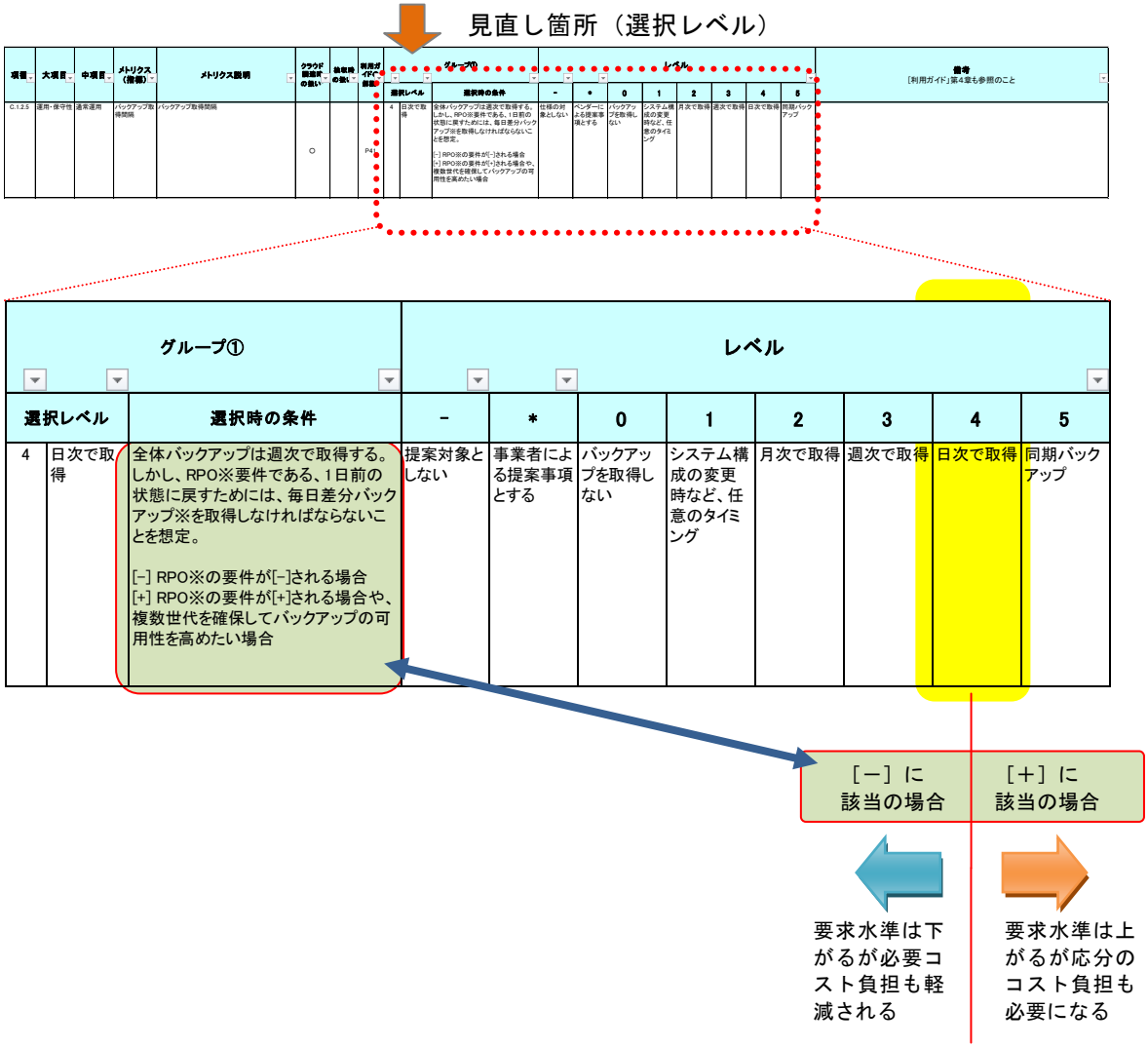
第６節　業務主管部門要求事項シートの作成

１　業務主管部門要求事項シートのレベル調整

非機能要件のうち、業務を遂行する立場から検討することが望まれる事項を検討する。「業務主管部門要求事項シート」の項目は、そのような性格の項目をまとめたものである。

選択レベルの中から、最もふさわしいレベルを設定する。シートには、「第５節　１　業務・情報システムグループの選択」で示した業務・情報システムの分類に応じて、実現性も考慮して、多くのケースで当てはまると考えられる選択レベルがあらかじめ設定してある。

調達対象となる情報システムや地方公共団体の実状に応じて、レベルを上げる、あるいは下げる必要がありえる。各活用シートの「選択時の条件」欄に記載された事項を考慮し、レベルを調整する。文頭に［＋］（プラス）と書かれた事項に該当する場合はレベルを上げることを検討する必要がある。反対に［－］（マイナス）と書かれた事項に該当する場合はレベルを下げることを検討する必要がある（図－13）。



図－ 13　レベル調整のイメージ

なお、レベルを上げた場合には、それに応じて必要コストも増加する可能性がある。コストを意識せず、あった方がいい、好ましいという考えで必要以上にレベルを上げてしまうと、費用対効果の得られない情報システムの調達を行うこととなったり、予算内での情報システムの調達を困難にするおそれがある。必要レベルを見極めるとともにコスト感覚を持ちながら、検討を行うことが重要である。最終的には、後述の実現方法要求事項シートと同様に、RFI（情報提供依頼）やベンダーへのヒアリング等を通じて、コスト（見積り）を始めとする情報を入手し判断する。

レベル調整に当たって、特に留意すべき項目については、各シートに記載しているほか、「第４章　レベル調整時の留意点」に示しているので、参照の上、検討する。

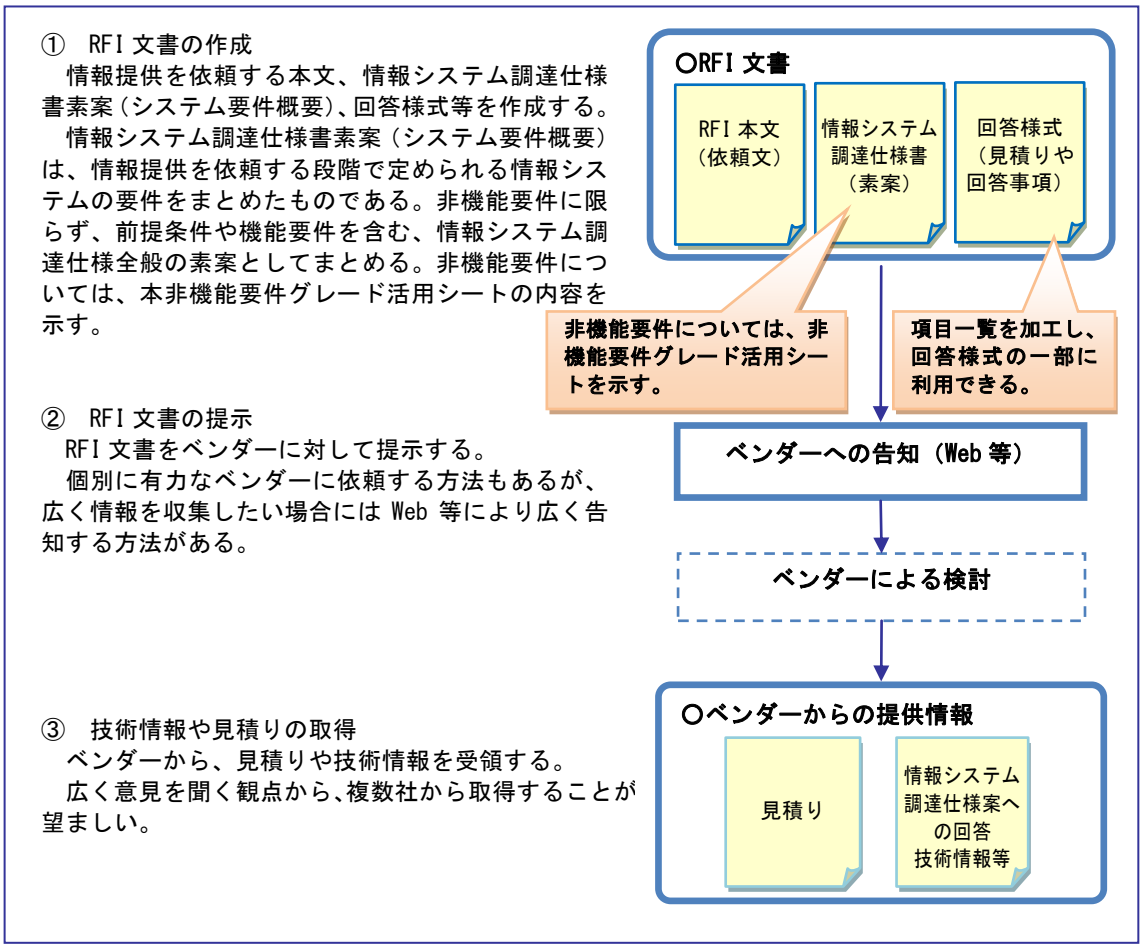
第７節 実現方法要求事項シートの作成

１　RFI 等の実施　　【主な実施者：ICT 部門若しくは業務主管部門】

「実現方法要求事項シート」は、技術的にどのような実現方法を採用するかという内容を含む要件項目である。本項目については、情報システムの設計思想の違い等もあることから、どのような方法を採用するのがよいかをベンダーに確認しながら検討することが有益な項目である。したがって、ベンダーに対して RFI（情報提供依頼）やヒアリング等を行い、選択レベルや、より具体的な実現方法等について、メリット・デメリットや必要コスト等を勘案しながら検討することを想定している。

シートに設定してある選択レベルについて、本シートに記載されていない情報システム調達仕様書の記載事項（第２章　図－5「非機能要求グレード（地方公共団体版）の情報システム調達仕様書の中での取扱範囲」を参照。）を示しながら、ベンダーに確認を行う。選択レベルを上下することが望ましいか、更に具体的な実現方法があるかについて、必要コストも含めて聴取を行う。

RFI の作業の流れの例を図－14 に示す。

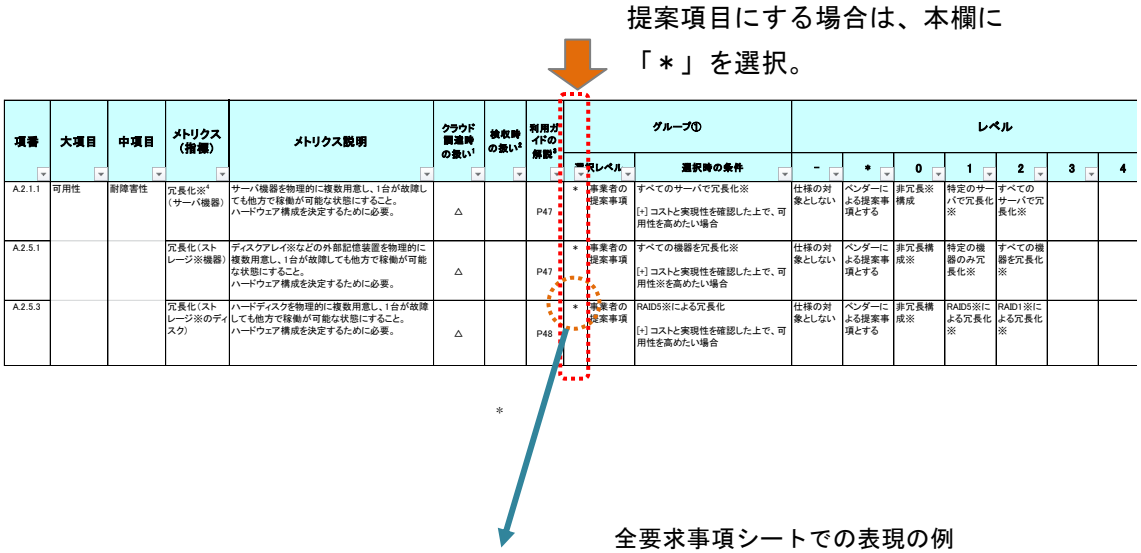


図－ 14　一般的な RFI 実施の流れ

2　実現方法要求事項シートのレベル調整　【主な実施者：ICT 部門若しくは業務主管部門】

ベンダーに対する RFI やヒアリングの結果を踏まえ、メリット・デメリット、実現性やコストの側面も加味して、最終的に採用する選択レベルを決定する。

なお、RFI やヒアリングを実施しても判断に迷う場合など、選択レベルを決定せず、ベンダーに提案を求める項目として扱う方法も考えられる。その場合には、「選択レベル」欄を数字ではなく「＊」を選択する。「＊」を選択すると、最終的に情報システム調達仕様書の基となる「全要求事項シート」において、提案項目であることが判別できるように表示される（図－15）。なお、活用シートでは、すべての項目で「＊」を選択することができるが、項目によっては、提案事項とすることがふさわしくないもの（例：E.1.1.1、F.1.1.1 等）もあるので、留意すること。



図－ 15　提案項目とする場合の設定方法

第８節 検討結果の情報システム調達仕様書への反映

１　非機能要件の確定　【主な実施者：業務主管部門】

ここまで各シートにおいて検討してきた非機能要件は、「全要求事項シート」にすべて反映されるようになっている。

非機能要求グレードでは、要件のレベルを抽象化した表現で示している。最終的にベンダーに示す要件にするため、一部の項目については具体化を図る必要がある。全要求事項シートの「規定事項の条件」には、見直しが必要な項目やどのように見直しをするかが示されている。また、具体的な情報システム調達仕様書の文案も「情報システム調達仕様書記載例」として示しているため、シートの記載内容に沿って見直し作業を行う。

見直しが必要な作業としては、表－6 に示すようなものがある。

表－ 6　非機能要件を明確化するための全要求事項シートを基にした見直し作業内容

見直し事項	見直し作業内容	例
数値化	数値条件についてレンジで示してあったり、抽象的に示されているものについて、具体的に数値化する。	B.1.1.1　ユーザ数 「上限が決まっている」 ↓ 〇〇〇人
対象の明確化	選択レベルの表現が「一部」となっているような事項について、対象を明確化する。	A.2.1.1　冗長化（サーバ） 「特定のサーバで冗長化」 ↓ 〇〇を冗長化
	定めた要件について、今回の調達対象でない機器や情報システムで実現する場合。	E.5.1.1　管理権限を持つ主体の認証 「複数回、異なる方式による認証」 ↓ 「本要件は、既存の〇〇により実現するので、〇〇と連携できるようにすること。」といった追記を行う。

２　検討結果の情報システム調達仕様書への反映　【主な実施者：業務主管部門】

全要求事項シートにまとめられた非機能要件について、情報システム調達仕様書に組み込み、情報システム調達仕様書として完成させる。組込み方としては、以下のような方法がある。

- 情報システム調達仕様書の本文では非機能要件は「別表参照」として、全要求事項シートをベースとした表を添付する。
- 情報システム調達仕様書本文の非機能要件の項目に、「全要求事項シート」のテキストをコピーアンドペーストし、整形する。

なお、活用シートでは、本利用ガイドの用語集で解説を加えた用語については「※」が付記されている。情報システム調達仕様書としてまとめる際には、「※」がついた用語について、情報システム調達仕様書にも同様に用語集を付け加えて補足するか、「※」を削除する。

非機能要求グレード（地方公共団体版）を利用して作成した情報システム調達仕様書についての著作権は、作成した各地方公共団体にある。したがって、特に、著作権者等の表示の必要はない。

ただし、活用シート自体を各地方公共団体において独自の変更等を行い、自らの著作物（二次的著作物）としてホームページで公表・発表する等外部に提供する場合には、各シートに記載されている［使用条件］に従って取り扱う必要がある。具体的には、以下のように取り扱う。

○［使用条件］の記載

活用シート等の［使用条件］の記載を表－7 の例に倣って変更の上、示すこと。

表－ 7　［使用条件］の記載例　　（○○○は各地方公共団体名）

1．　本資料の著作権は、独立行政法人情報処理推進機構、財団法人地方自治情報センター及び○○○が保有しています。
2．　本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものを基に、○○○が一部変更したものです。
3．　独立行政法人情報処理推進機構、財団法人地方自治情報センター及び○○○は、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。
4．　独立行政法人情報処理推進機構、財団法人地方自治情報センター及び○○○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、財団法人地方自治情報センター及び○○○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、財団法人地方自治情報センター又は第三者の著作権、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、財団法人地方自治情報センター及び○○○は、本資料のシステム開発への利用、開発された情報システムの使用、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、○○○までご連絡下さい。

○活用シートのコピーライトの記載

活用シートのフッターにあるコピーライトの記載を表－8 の例に倣って変更の上、示すこと。

表－ 8　コピーライトの記載例　　○○○は各地方公共団体名

Copyright © 2010-2014 IPA，LASDEC，○○○

第４章 レベル調整時の留意点

レベル調整をするに当たり、コストに大きく影響が出る、選択レベルが複雑なものなど、特に留意すべき項目について、その留意点や判断のポイントを以下に示す。

第１節 全庁的要求事項シート

全庁的要求事項シートに含まれる項目は、個々の情報システム単位ではなく、一般に庁内の規定（例：情報セキュリティポリシー）や全庁的な情報システム環境（例：ネットワークや情報セキュリティ）に基づいて調整すべきものを選んであるため、各地方公共団体の実状に応じて設定すること。

C.2.3.5 OS 等パッチ適用タイミング

OS やミドルウェア、その他のソフトウェア（以下「OS 等」という。）のパッチの適用のタイミングについて定める。パッチの適用は緊急性の高いセキュリティ対応のものは、迅速に適用することが望ましい。ただし、緊急性の少ないものまで頻繁に適用を行うと適用作業や検証のためのコストが発生することに留意が必要である。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM[4]の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。

表－ 9 OS 等パッチ適用タイミングに関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	パッチを適用しない	OS 等パッチを一切適用しない場合に選択する。 環境を一切変えることが許されない等、特殊なケースの場合に選択する。
レベル１	障害発生時にパッチ適用を行う	障害等が発生した際に、OS 等パッチの適用を行う場合に選択する。
レベル２	定期保守時にパッチ適用を行う	定期保守時に OS 等パッチの適用を行う場合に選択する。 定期保守までの間は、脆弱性によって生じる可能性のあるリスクを受容する必要がある。
レベル３	緊急性の高いパッチのみ即時に適用を行う。	緊急性の高い情報セキュリティ対策の OS 等パッチのみ即時に適用する場合に選択する。 セキュリティ対策を考慮すると、通常はこのレベル以上の選択が望ましい。
レベル４	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高い情報セキュリティ対策の OS 等パッチは即時に適用し、それ以外の緊急性の高くない OS 等パッチは定期保守時に適用を行う場合に選択する。

[4] Service Level Management の略。IT サービスなどで、サービスの品質について継続的に点検・検証を行い、品質の維持や改善を図ること。

レベル	設定値	設定時の考え方や留意点
レベル５	新規のパッチがリリースされるたびに適用を行う	新規のパッチがリリースされる都度、即時に OS 等パッチの適用を行う場合に選択する。

C.4.4.1　リモート監視地点

情報システムの設置場所から離れた場所より監視を行うかどうかを定める。リモート監視を行った場合には、ベンダーの拠点から監視が可能であり常駐等の必要がなくなるため、対応の迅速性を高めながら運用・保守コストを低減することができる。一方で、情報セキュリティ面でのリスクが生じることに留意すること。

表－ 10　リモート監視地点に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	リモート監視を行わない	リモート監視を行わない場合に選択する。
レベル１	庁内LANを介してリモート監視を行う	庁内LANの接続された拠点から監視を行う場合に選択する。庁内の一ヶ所の拠点から、情報システムやネットワーク全体を監視することができる。
レベル２	ベンダー拠点等外部からリモート監視を行う	ベンダー拠点等、外部からリモート監視を行う場合に選択する。 外部から庁内の情報システムやネットワークに接続することになるので、利用するネットワークやベンダーの契約面等での情報セキュリティ対策の検討が必要となる。

C.4.4.3　リモート操作時の接続方法

ベンダーがリモート監視地点から情報システムのリモート操作を実施する場合の回線接続方法を定める。リモート操作において実施可能な操作や、リモート操作開始及び終了の連絡等については、運用開始前にあらかじめ明確化する必要がある。リモート操作を行った場合には、ベンダーの拠点から保守対応や運用が可能であり、常駐等の必要がなくなるため、対応の迅速性を高めながら運用・保守コストを低減することができる。一方で、回線を利用するためのコストが発生することに留意すること。

表－ 11　リモート操作の範囲に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	リモート操作を行わない	リモート操作を行わない場合に選択する。
レベル１	リモート操作の必要時のみ接続する	公衆回線等により、リモート操作の必要時のみ接続を行う場合に選択する。
レベル２	常時接続環境にてリモート操作を行う	専用回線等により、常時接続した環境にて、リモート操作を行う場合に選択する。

E.4.3.4　ウィルス定義ファイル適用タイミング

ウィルス対策ソフトのウィルス定義ファイルの適用について、いつ実施するかを定め

る。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。

表－ 12　ウィルス定義ファイル適用タイミングに関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	定義ファイルを適用しない	定義ファイルを適用しない場合に選択する。ウィルス対策ソフトを導入した場合、定義ファイルを適用しないことは考えにくいので、通常は選択しない。
レベル１	定期保守時に実施	定期保守時にウィルス定義ファイルの適用を実施する場合に選択する。
レベル２	定義ファイルリリース時に実施	定義ファイルリリースがあった際に、即時に適用する場合に選択する。情報セキュリティ確保の観点から、通常は、このレベルを選択する。即時に適用できるよう自動的に適用する仕組みを整備することが一般的である。

E.5.1.1　管理権限を持つ主体の認証

業務や情報システムの管理者について、認証の回数や方法等、認証をどれだけ厳しく行うかを選択する。全庁的な認証基盤があり、それを利用する場合には、その点を踏まえて調整を行うとともに、そのことを要件に付記する（例：「IC カードによる認証は、既存の IC カード及び認証基盤により行う。当該認証基盤と連携して実現すること」）。

どのレベルを選択するかは、各地方公共団体の情報セキュリティポリシーに従い、リスクを考慮して決定する。

表－ 13　管理権限を持つ主体の認証に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	実施しない	認証を特に実施しない場合に選択する。
レベル１	1 回	ID/パスワード等の方法により、ログイン時に 1 度だけ認証すればよい場合に選択する。
レベル２	複数回の認証	ID/パスワード等の方法により、複数回認証を必要とするときに選択する。 例えば、ネットワークの利用のログイン時に 1 回、更に情報システム利用時に個別に 1 回の認証を必要とするような場合に選択する。
レベル３	複数回、異なる方式による認証	ID/パスワード等に加え IC カードによる認証の両方を行う等、複数の方式を組み合わせて認証を行う場合に選択する。 例：全庁的な認証基盤では IC カードにより認証を行い、更に対象となる情報システムの利用時には ID/パスワードによる認証を行うなど。

E.6.1.1　伝送データの暗号化の有無

当該システムのデータを庁内 LAN 等で伝送する際に、暗号化するかどうかを選択する。なお、暗号化を実現する機器や情報システムが対象となる情報システムの調達対象

ではなく、既存の機器や情報システムを利用して実現する場合には、その旨を参考情報として示す。

どのレベルを選択するかは、各地方公共団体の情報セキュリティポリシーに従い、リスクを考慮して決定する。

表－ 14　伝送データの暗号化の有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	無し	特に暗号化は行わない場合。
レベル１	認証情報のみ暗号化	パスワード等の認証情報のみを暗号化して伝送する場合。
レベル２	重要情報を暗号化	重要情報についてはすべて暗号化して伝送する場合。
レベル３	すべてのデータを暗号化	伝送の対象となるデータはすべて暗号化して伝送する場合。

E.6.1.2　蓄積データの暗号化の有無

当該システムの蓄積データを暗号化するかどうかを選択する。

どのレベルを選択するかは、各地方公共団体の情報セキュリティポリシーに従い、リスクを考慮して決定する。

表－ 15　蓄積データの暗号化の有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	無し	特に暗号化は行わない場合。
レベル１	認証情報のみ暗号化	パスワード等の認証情報のみを暗号化して蓄積する場合。
レベル２	重要情報を暗号化	重要情報についてはすべて暗号化して蓄積する場合。 対象となる重要情報の種類やバックアップ等外部記録媒体のみを行うのか、サーバ上のデータも暗号化するのかについても検討を行う。 暗号化を行うと処理速度に影響が出たり、障害時の復旧に支障が出るおそれもあるので、考慮すること。

E.10.1.1　セキュアコーディング、Web サーバの設定等による対策の強化

Web 技術を利用した情報システムで、特に、外部向けの情報システムの場合について、情報セキュリティ対策を強化するかどうかを検討する。

外部向けの Web 技術を利用した情報システムについては、悪意のあるコードを埋め込まれたり、乗っ取られたりするリスクがあるため、対策を施すことが望ましい。詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」[5]を参照の上、対策を検討する。

なお、パッケージソフトウェアを使用する場合には、セキュアコーディングに対応し

---

[5] 財団法人地方自治情報センター「『地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）』を一般公開しました」＜https://www.lasdec.or.jp/cms/12,28369,84.html＞（最終アクセス平成 26 年 2 月 5 日）

ていない場合もあるため、複数ベンダーに実現の可能性を確認することを推奨する。

表－ 16　セキュアコーディング、Web サーバの設定等による対策の強化に関する
レベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	無し	セキュアコーディング、Web サーバの設定等による対策の強化を行わない場合に選択する。 外部向けの Web システムの場合には、対策の強化が望ましく、レベル 0 は極力選択しないことが望ましい。
レベル１	対策の強化	セキュアコーディング、Web サーバの設定等による対策の強化を行う場合に選択する。 外部向けの Web システムの場合には、極力選択することが望ましい。

E.10.1.2　WAF の導入の有無

WAF（Web Application Firewall）の設置の有無について定める。WAF はウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するためのセキュリティ対策である。WAF についての詳細は、IPA の「Web Application Firewall 読本」[6]が参考になる。

表－ 17　 WAF の導入の有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	無し	WAF を導入しない場合に選択する。 Web システムでない場合や特に攻撃に備える必要がない情報システムの場合に選択する。
レベル１	有り	WAF を導入する場合に選択する。 特に攻撃に備える必要がある情報システムについて導入を考慮する。

F.3.1.1　規格取得の有無（安全性）

機器等についての安全性について、各地方公共団体の規則等に従って、規格・認証の取得を求める内容について定める。UL（Underwriters Laboratories Inc.）認証は、米国の安全規格であり、各国にも同様な規格がある。国内では 454 品目の電気製品について、電気製品安全法の対象となるが、コンピュータ機器総体としては同法の対象とはなっていない。

表－ 18　規格取得の有無（安全性）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規格取得の必要無し	特に安全性についての規格・認証を求めない場合に選択する。

[6]IPA「Web Application Firewall 読本」＜http://www.ipa.go.jp/security/vuln/waf.html＞（最終アクセス平成 26 年 2 月 5 日）。

レベル	設定値	設定時の考え方や留意点
レベル１	規格取得の必要有り	安全性についての規格・認証を求める場合に選択する。 情報システム調達仕様書では、対象となる機器等や規格についても明示する必要がある。

F.3.2.1　規格取得の有無（有害物質）

電子機器等の有害物質の使用制限について、各地方公共団体の規則等に従って、規格・認証の取得を求める内容について定める。EU では、RoHS 指令以外に、REACH（Registration, Evaluation, Authorization and Restriction of Chemicals(1907/2006)）規則を定めている。

これは、2007 年 6 月に発効した、化学物質の総合的な登録、評価、認可、制限の制度であり、対象は電子機器に限らず、化学物質もより広範に定めている。なお、メーカーの中には、このような指令や規則に準拠した自主的な基準を策定し、出荷しているところもある。

表－ 19　規格取得の有無（有害物質）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規格取得の必要無し	特に有害物質についての規格・認証を求めない場合に選択する。
レベル１	RoHS 指令相当取得	有害物質についての規格・認証を求める場合に選択する。 情報システム調達仕様書では、対象となる機器等や規格についても明示する必要がある。

F.5.1.1　グリーン購入法対応度

各地方公共団体の環境対策の方針や規則等に従って、当該システムで扱う機器等において、グリーン購入法等、環境面で考慮するかどうかを選択する。

表－ 20　グリーン購入法対応度に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	対処不要	当該システムで扱う機器等において、特にグリーン購入法の対応等を求めない場合に選択する。
レベル１	グリーン購入法の基準を満たす製品を一部使用	当該システムで扱う機器等において、一部の機器について特にグリーン購入法等の対象にする場合に選択する。また、どの機器をその対象とするかを明確にする。
レベル２	グリーン購入法の基準を満たす製品のみを使用	当該システムで扱う機器において、すべての機器について特にグリーン購入法等に対象とする場合に、選択する。

第２節 業務主管部門要求事項シート

A.1.3.1 RPO（目標復旧地点）（業務停止時）

RPO（目標復旧地点）とは、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情報システムをどの時点まで復旧するかを定める目標値である。目標復旧地点を短くするほど、データ復旧時の対応負担は減るが、コストは増加する。

なお、ICT-BCP を策定している地方公共団体で、障害時における RPO を設定している場合においては、ICT-BCP で規定した目標に沿って選択する。ICT-BCP については、総務省「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」（平成 20 年 8 月）[7]、総務省「ICT-BCP 初動版 導入ガイド」（平成 25 年 5 月）[8]等を参照すること。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 21　RPO（目標復旧地点）（業務停止時）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	復旧不要	障害発生時に、特に復旧を必要としない場合。
レベル１	5 営業日前の時点（週次バックアップからの復旧）	バックアップは週単位になる。週間の異動量が少なく、週単位であれば手作業で復旧可能な場合に選択する。
レベル２	1 営業日前の時点（日次バックアップからの復旧）	バックアップは日単位になる。週間の異動量は多く手作業での対応は困難だが、日単位であれば復旧可能な場合に選択する。
レベル３	障害発生時点（日次バックアップ+アーカイブからの復旧）	バックアップは障害発生時点となる。毎日の異動量が多く、日単位でも手作業では復旧対応困難な場合に選択する。

A.1.3.2 RTO（目標復旧時間）（業務停止時）

RTO（目標復旧時間）業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する時間を目標として定めるものである。

なお、ICT-BCP を策定している地方公共団体で、障害時における RTO を設定している場合においては、ICT-BCP で規定した目標に沿って選択する。また、あらゆる条件下においても達成する必要のある目標とするとコスト高になるので、障害の条件を限定することも考えられる。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

---

[7]総務省「電子自治体の推進」＜http://www.soumu.go.jp/denshijiti/＞（最終アクセス平成 26 年 2 月 5 日）。
[8]総務省「電子自治体の推進」＜http://www.soumu.go.jp/denshijiti/＞（最終アクセス平成 26 年 2 月 5 日）。

表－ 22　RTO（目標復旧時間）（業務停止時）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	1 営業日以上	障害の際、数日間、情報システムが停止しても許される場合に選択する。
レベル１	1 営業日以内	障害の際、翌日中に、情報システムが再開すれば許される場合に選択する。
レベル２	12 時間以内	障害の際、その日のうちに、情報システムが再開すれば許される場合に選択する。
レベル３	6 時間以内	障害の際、その日の業務時間内には、情報システムの再開が求められる場合に選択する。 このレベルを選択した場合、厳重なシステム構成や体制が必要となるため、相応のコストが発生する可能性があることに留意が必要となる。
レベル４	2 時間以内	障害の際、窓口業務等で、情報システムは極力止められない場合に選択する。 このレベルを選択した場合、厳重なシステム構成に加え、即応できる体制が必要となるため、相当のコストが発生する可能性があることに留意が必要となる。 人的対応が必要となるため、近隣にベンダーの拠点がない場合は、対応が難しい場合がある。

A.1.3.3　RLO（目標復旧レベル）（業務停止時）

RLO（目標復旧レベル）は、業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべての情報システム機能）の目標値である。

なお、ICT-BCP を策定している地方公共団体で、障害時における RLO を設定している場合においては、ICT-BCP で規定した目標に沿って選択する。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 23　RLO（目標復旧レベル）（業務停止時）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規定しない	障害の際の復旧レベルについて考慮せず、規定しない場合に選択する。
レベル１	一部システム機能の復旧	障害の際、当面は、情報システムの機能全体ではなく、窓口における証明書発行機能のみ、表示・参照機能のみ等、限定した機能のみ復旧すればよい場合に選択する。 A.1.3.2 RTO で設定する値は、この一部システム機能を復旧するまでの時間を表す。 全システム機能を復旧するより対策がしやすくなり、現実的な要件として示せる場合がある。 仕様では、復旧する情報システム機能を明らかにする。
レベル２	全システム機能の復旧	障害の際、直ちにすべての情報システム機能を復旧する場合がある場合に選択する。 全システム機能の復旧を行うために、一部システム機能の復旧に比べ、コスト高となる。

A.1.4.1　システム再開目標（大規模災害時）

システム再開目標（大規模災害時）は、大規模災害が発生した際、どれくらいの期間で情報システムを復旧させるかの目標である。ここでは、最低限の業務を実施できる水準で情報システム機能や性能を提供することを前提に目標を設定する（平常時と同等の水準の機能や性能を提供することを前提とすると、短期間での復旧が不可能になったり、高額なコストが必要となるため、それを前提としない）。

また、情報システム調達仕様書では、情報システムの稼働に必要な調達対象外の資源（例：電力や通信、施設等）についての確保状況についても、要件の前提として示す必要がある（再開に当たっては、これらの資源は確保されている必要がある）。

なお、ICT-BCP を策定している地方公共団体においては、ICT-BCP で規定した目標に沿って選択する。

また、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 24　システム再開目標（大規模災害時）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	再開不要	災害時には再開が不要の場合に選択する。
レベル１	数ヶ月以内に再開	災害時に、数ヶ月以内に再開すればよい場合に選択する。
レベル２	一ヶ月以内に再開	災害時に、一ヶ月以内に再開すればよい場合に選択する。
レベル３	一週間以内に再開	災害時に、一週間以内に再開する必要がある場合に選択する。 このレベルは、厳しい条件であり、ベンダーに実現可能性も含めて確認をする必要がある。
レベル４	3 日以内に再開	災害時に、3 日以内に再開する必要がある場合に選択する。 このレベルは、かなり厳しい条件であり、ベンダーに実現可能性も含めて確認をする必要がある。
レベル５	1 日以内に再開	災害時に、1 日以内に再開する必要がある場合に選択する。 このレベルは、非常に厳しい条件であり、ベンダーに実現可能性も含めて確認をする必要がある。

A.1.5.1　稼働率

稼働率（サービス稼働率と同義）は、表－25 のとおり計算される。

表－ 25　稼働率の計算式

○サービス稼働率　　＝　[実サービス稼動時間]　／　[サービス提供時間] ○サービス提供時間　＝　[契約サービス時間]　－　[事前通知された定期保守によるサービス停止時間]

出所：総務省「地方公共団体における ASP･SaaS 導入活用ガイドライン」,平成 22 年 4 月,p.58 [9]

実サービス稼働時間とは、情報システムが停止せずにサービスを提供した累計の時間である。ベンダーとの契約に当たっては、情報システムが停止した時間に、情報システムの部分的な停止（端末の故障やネットワークの停止による拠点別の停止）時間を除くか、天災やベンダー以外の要因による停止時間を除くか等の条件について合意する必要がある。また、契約サービス時間とは、ベンダーが情報システムを稼働させる時間として契約において約束する時間である（C.1.1.1/C.1.1.2 運用時間とは必ずしも同じではない）。通常、業務に利用する時間のほか、バッチ処理やバックアップ処理等を実施する時間が含まれるが、様々な捉え方がある。稼働率の計算に当たって、どこまで含むかについて、ベンダーと合意する必要がある。

情報システムの稼働率は 100%、すなわち、停止時間はゼロであることが望ましいと考え、要件として示しがちであるが、情報システムの停止を皆無にすることは困難であり、停止時間を短くしようとすると、そのための対策（情報システム面や体制面）にコストが伴う。年間にどのくらいの停止が許容できるかを勘案し、費用対効果も考えて合理的な値を設定することが重要である。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 26　稼働率に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル 0	規定しない	特に稼働率の要件を規定しない場合に選択する。
レベル 1	95%	1 日 12 時間で平日（242 日）稼働する情報システムにおいて、年間 145 時間程度の停止（事前に通知のあった定期保守による停止時間は除く。以下同様）が許される情報システムの場合に選択する。

[9]総務省「『地方公共団体における ASP･SaaS 導入活用ガイドライン』の公表及び意見募集の結果」＜http://www.soumu.go.jp/menu_news/s-news/02gyosei07_000026.html＞（最終アクセス平成 26 年 2 月 5 日）。

レベル	設定値	設定時の考え方や留意点
レベル２	99%	1 日 12 時間で平日（242 日）稼働する情報システムにおいて、年間累計 29 時間程度の停止が許される情報システムの場合に選択する。
レベル３	99.5%	1 日 12 時間で平日（242 日）稼働する情報システムにおいて、年間累計 14.5 時間程度の停止が許される情報システムの場合に選択する。
レベル４	99.9%	1 日 12 時間で平日（242 日）稼働する情報システムにおいて、年間累計 2.9 時間程度の停止が許される情報システムの場合に選択する。 比較的厳しい条件であり、相応のコストが必要である。
レベル５	99.99%	1 日 12 時間で平日（242 日）稼働する情報システムにおいて、年間累計 17 分程度の停止が許される情報システムの場合に選択する。 非常に厳しい条件であり、高額のコストが必要である。 地方公共団体の情報システムで設定されることは稀と考えられる。

B.2.1.4　通常時オンラインレスポンスタイム

オンラインレスポンスタイムは、処理の実行指示を与えてから最初の応答を得るまでにどのくらいの時間がかかるのかを表すものである。できるだけ速い方がよいと考えがちであるが、短くすればするほどコストが必要となる。業務上の利用場面を想定し、どの程度であれば許容できるかを勘案して選択する。

通常時オンラインレスポンスタイムは、すべての操作や、特殊な条件においても必ずこの時間内に処理が終了することを求めるものではない。どのような画面や操作によるものか、どこまでの処理（通常の画面展開、検索等）を含むものなのか、ネットワークの影響についてどのように扱うか等の測定の条件についても、要件に付随する条件として明確化する。あるいは、ベンダーに提案を求めそれを基に協議を行うことにより、ベンダーと合意することが望ましい。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 27　通常時オンラインレスポンスタイムに関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規定しない	特に操作上の速度を求めない場合に選択する。
レベル１	10 秒以内	操作時間にある程度余裕を持たせることができる場合に選択する。
レベル２	5 秒以内	業務の特性上、操作の待ち時間に余り余裕を持たせることができない場合に選択する。 比較的高度なシステム構成が必要となり、相応のコストが発生するので、留意が必要である。

レベル	設定値	設定時の考え方や留意点
レベル３	3 秒以内	業務の特性上、操作の待ち時間に余裕を持たせることができない場合に選択する。 高度なシステム構成が必要となり、高額なコストが発生するので、留意が必要である。
レベル４	1 秒以内	業務の特性上、操作の待ち時間に全く余裕を持たせることができない場合に選択する。 非常に高度なシステム構成が必要となり、非常に高額なコストが発生するので、留意が必要である。地方公共団体の情報システムで選択されることは非常にまれである。

B.2.1.5　アクセス集中時のオンラインレスポンスタイム

アクセス集中時のオンラインレスポンスタイムは、対象となる情報システムに、想定される最大限のアクセスが集中した条件下において、処理の実行指示を与えてから最初の応答を得るまでにどのくらいの時間がかかるのかを表すものである。

設定に当たっての考え方は B.2.1.4 と同様であるが、付随する条件として、アクセス集中時とは、どのような状態（○○ユーザが同時にアクセスする等）を指すかをできる限り明確に示すことが望ましい。アクセス集中時の要件であるので、通常時に比べて条件としてはより厳しくなることに留意が必要である。

C.1.1.1　運用時間（平日）

運用時間（平日）は、業務主管部門等の利用者が業務のために情報システムを利用する時間を指す。バッチ処理やバックアップ処理等のためにサーバを立ち上げている時間とは異なる。

表－ 28　運用時間（平日）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規定無し（不定期利用）	特に情報システムの稼働を保証すべき運用時間を定めない場合に選択する。
レベル１	定時内での利用 （1 日 8 時間程度利用）	通常の業務（開庁）時間内において利用する場合に選択する。ベンダー側の対応も業務時間内となるので、費用も一定額に収まる。
レベル２	定時外も頻繁に利用 （1 日 12 時間程度利用）	通常の業務（開庁）時間に加えて、残業時間帯においても利用する場合に選択する。ベンダーの対応も時間外対応となるため、その分のコストが増加する。
レベル３	24 時間利用	24 時間利用する場合に選択する。ベンダーの対応も 24 時間運用を前提とするため、コストが増加する。

C.1.1.2　運用時間（休日等）

運用時間（休日等）は、土日、祝祭日や年末年始等の休日においての運用時間を指す。設定に当たっての考え方は、C.1.1.1 運用時間（平日）と同様である。ただし、休日のため、レベルを上げると、よりコストが増加することに留意が必要である。

表－ 29　運用時間（休日）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	規定無し（原則利用しない）	原則的に休日には情報システムを運用しない場合に選択する。
レベル１	定時内での利用（1 日 8 時間程度利用）	通常の業務（開庁）時間内において利用する場合に選択する。ベンダー側の対応も業務時間内となるので、費用も一定額に収まる。
レベル２	定時外も頻繁に利用（1 日 12 時間程度利用）	通常の業務（開庁）時間に加えて、残業時間帯においても利用する場合に選択する。ベンダーの対応も時間外対応となるため、その分のコストが増加する。
レベル３	24 時間利用	24 時間利用する場合に選択する。ベンダーの対応も 24 時間運用を前提とするため、コストが増加する。

C.1.2.5　バックアップ取得間隔

どのくらいの頻度でバックアップを取得するかを選択する。頻度が高いほど、データ復旧時の作業量を減らすことができるが、相応のコストが発生する。

「A.1.3.1　RPO(目標復旧地点)(業務停止時)」とも整合がとれたレベルを選択する。

表－ 30　バックアップ取得間隔に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	バックアップを取得しない	特にバックアップの取得が必要でない場合に選択する。
レベル１	システム構成の変更時など、任意のタイミング	普段は、バックアップは不要だがシステム構成の変更時（システム更改時を含む）等においてのみバックアップが必要、あるいはデータの異動が年 1 回等ある決まった時点で発生し、その時点でバックアップを取得すればよい場合に選択する。 仕様では、バックアップの取得のタイミングを明確にする。
レベル２	月次で取得	月間のデータの異動量が余り多くない場合等、バックアップデータからのデータ復旧が月単位でよい場合に選択する。
レベル３	週次で取得	RPO が「5 営業日前の時点」の場合、その要件を満たすためにバックアップデータからのデータ復旧が週単位で必要な場合に選択する。
レベル４	日次で取得	RPO が「1 営業日の前の時点」の場合、その要件を満たすためにバックアップデータからのデータ復旧が日単位で必要な場合に選択する。 なお、この場合、通常、全体バックアップは週次、差分バックアップを日次で取得することが多い。
レベル５	同期バックアップ	RTO が数時間程度と短い場合、その要件を満たすためにリアルタイムでバックアップを取得する必要がある場合に選択する。 レベル 4 に比べて、情報システムの資源が必要なため、相応のコストが発生する。

C.3.3.2　駆けつけ到着時間

情報システムの異常を検知した場合に、保守員が現地対応のためにどのくらいの迅速さで駆けつけるかを定める。短くなればなるほど、ベンダー側でそのための体制を用意しておく必要があるため、コストが増加することに留意する必要がある。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 31　駆けつけ到着時間に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	保守員の駆けつけ無し	職員が対応する等、保守員が特に駆けつける必要がない場合に選択する。
レベル１	保守員到着が異常検知から数日中	業務の特性上、現地対応までに数日かかってもよい場合に選択する。
レベル２	保守員到着が異常検知からユーザの翌営業日中	業務の特性上、現地対応が、翌日になってもよい場合に選択する。
レベル３	保守員到着が異常検知からユーザの翌営業開始時まで	業務の特性上、翌日の業務開始時点までに到着し、現地対応を開始する必要がある場合に選択する。 ベンダー側で相応の体制を整える必要があり、そのためのコストが必要となる。
レベル４	保守員到着が異常検知から数時間内	業務の特性上、数時間以内に到着し、現地対応を開始する必要がある場合に選択する。 ベンダー側で常に対応できる体制を整える必要があり、そのためのコストが必要となる。 なお、近隣にベンダーの拠点がない場合は、対応が難しい場合がある。
レベル５	保守員が常駐	業務の特性上、保守員が現地に常駐し、常に対応できる体制が必要な場合に選択する。 常駐人員の人件費コストが生じ、保守費用が増加することに留意する。

C.3.3.4　障害検知通知時間

障害検知通知時間は、システム障害が発生した際、ベンダーが、地方公共団体に障害発生時点から障害を通知するまでの時間を意味している。特にクラウドやベンダーのデータセンター等により情報システムを運用している場合に必要となる要件である。短くなればなるほど、ベンダー側でそのための体制を用意しておく必要があるため、コストが増加することに留意する必要がある。

なお、本項目の検収の扱いとしては、継続的に評価を行う対象として取り扱うことが考えられる。SLM の考え方で継続的な評価を行いながら、その水準の維持・向上を図るよう運用することが望まれる。情報システム調達仕様書にも「○○を目標とする」「およそ○○とする」等、目標値である旨の表記をすることも考慮する。

表－ 32　障害検知通知時間に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	障害を検知しない	特にベンダー側で障害の検知を行う必要がない場合に選択する。
レベル１	24 時間以内	業務の特性上、ベンダーの障害検知から 24 時間以内には職員（通常、情報システム担当者）に通知の必要がある場合に選択する。
レベル２	８時間以内	業務の特性上、ベンダーの障害検知から 8 時間以内には職員（通常、情報システム担当者）に通知の必要がある場合に選択する。
レベル３	３時間以内	業務の特性上、ベンダーの障害検知から 3 時間以内には職員（通常、情報システム担当者）に通知の必要がある場合に選択する。
レベル４	１時間以内	業務の特性上、ベンダーの障害検知から 1 時間以内には職員（通常、情報システム担当者）に通知の必要がある場合に選択する。 特に職員が通常利用していないため異常を検知できない対住民向けの情報システム等で、地方公共団体側が障害等を早期に把握する必要がある場合に選択する。 情報システムをほぼ常時監視し、早期に連絡できる体制が必要になるため、コストが増加することに留意する。
レベル５	30 分以内	業務の特性上、ベンダーの障害検知から 30 分以内に職員（通常、情報システム担当者）に通知の必要がある場合に選択する。 特に職員が通常利用していないため異常を検知できない対住民向けの情報システム等で、地方公共団体側が障害等を直ちに把握する必要がある場合に選択する。 情報システムを常時監視し、すぐに連絡できる体制が必要になるため、コストが増加することに留意する。

C.5.1.2　保守契約（ハードウェア）の種類

保守契約（ハードウェア）の種類は、機器の故障時にどのような対応を求めるかについて定めるものである。レベルが上がるほど、機器の故障による影響を少なくすることができるが、ベンダー側の保守体制を必要とするので、コストが増えることに留意する。

表－ 33　保守契約（ハードウェア）の種類に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	保守契約を行わない	保守サービスが必要でない場合に選択する。
レベル１	随時保守 （センドバック）	故障等が発生した際に、ベンダー側に機器等を送付し、修理対応等を行い、都度費用を支払うような保守サービス。 機器の修理中は機器が使用できないため、代替機等がない場合には情報システムの運用に影響が出る。このような対応で許容できる場合に選択する。 一般的にコストが低減できる（故障頻度が高い場合には、定額保守に比べて割高になる場合もある）。

レベル	設定値	設定時の考え方や留意点
レベル２	定額保守 （センドバック）	故障等が発生した際に、ベンダー側に機器等を送付し、修理対応等を行う。あらかじめ契約の上、定額の費用を支払、定められた範囲で何度でも保守サービスを受けることができる。機器の修理中は機器が使用できないため、代替機等がない場合には情報システムの運用に影響が出る。このような対応で許容できる場合に選択する。 故障が発生しなくても費用が発生するため、一般的には割高になる（故障頻度が高い場合には、随時保守より安価で済む可能性もある）。
レベル３	随時保守 （オンサイト）	故障等が発生した際に、ベンダー側が現地を訪問し、修理対応等を行う。このため、機器故障による影響を小さくしたい場合に選択する。 センドバックに比べてベンダーが訪問する人件費分のコストが割高となる。 ただ、一般的に定額保守に比べてコストが低減できる（故障頻度が高い場合には、割高になる場合もある）。
レベル４	定額保守 （オンサイト）	故障等が発生した際に、ベンダー側が現地を訪問し、修理対応等を行う。このため、機器故障による影響を小さくしたい場合に選択する。 センドバックに比べてベンダーが訪問する人件費分のコストが割高となる。また、故障が発生しなくても費用が発生するため、一般的には割高になる（故障頻度が高い場合には、随時保守より安価で済む可能性もある）。

C.5.3.1　ライフサイクル期間

調達する情報システムについて、どのくらいの期間、稼働させるかについて選択する。短いと償却費用やリース料が割高となり、長いと保守部品の確保等の必要性から割高となったり、対応できるベンダーが限られることに留意する必要がある。

表－ 34　ライフサイクル期間に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	3 年	当該システムの稼働から稼働終了までを 3 年で計画する場合に選択する。 3 年は、一般的なハードウェアの耐用年数より短く、償却費用やリース料が割高になることに留意する。
レベル１	5 年	当該システムの稼働から稼働終了までを 5 年で計画する場合に選択する。 5 年は、標準的なハードウェアの保守対応期間であり、5 年で選択することが多い。
レベル２	7 年	当該システムの稼働から稼働終了までを 7 年で計画する場合に選択する。 7 年は、標準的なハードウェアの保守対応期間より長く、6 年目、7 年目は保守費用が割高になる場合がある。

D.3.1.1　設備・機器の移行内容

調達する情報システムが新規開発でなく再構築する場合に、その移行の対象を明らかにする。

表－ 35　設備・機器の移行内容に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	移行対象無し	移行する対象が特にない場合に選択する。
レベル１	移行対象設備・機器のハードウェアを入れ替える	ハードウェアのみの更改の場合に選択する。
レベル２	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	ハードウェアと、OS やミドルウェアを更改（バージョンアップ）する場合に選択する。
レベル３	移行対象設備・機器のシステム全部を入れ替える	ハードウェア、OS やミドルウェア、アプリケーションを含め、すべて再構築する場合に選択する。
レベル４	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する	ハードウェア、OS やミドルウェア、アプリケーションを含め、すべて再構築すると同時に、関連する情報システムと統合化を図る場合に選択する。

D.4.1.1　移行データ量

調達する情報システムが新規開発でなく再構築する場合に、その移行の対象となるデータの量を明らかにする。レベル設定時には、目安としての量を設定する。

表－ 36　移行データ量に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	移行対象無し	旧システムから新システムに移行する対象データが特にない場合に選択する。
レベル１	1TB 未満	移行する対象データが 1TB（テラバイト）未満の場合に選択する。
レベル２	10TB 未満	移行する対象データが 1TB 以上 10TB 未満の場合に選択する。
レベル３	10TB 以上	移行する対象データが 10TB 以上の場合に選択する。

F.2.5.1　特定製品の採用有無

オープンソース製品や、独立系ソフトウェア会社や独立系ハードウェア会社などの特定製品を採用するかどうかを示す。特定製品を指定した場合には、ベンダーのサポートの難易度が上がるため、コストが増加したり、対応できるベンダーが限られる可能性があるため留意が必要である。技術的理由（他に代わる製品がない等）、政策的な理由（オープンソースの利用を推進している等）、制度的な理由（国が指定している等）がある場合を除き、調達の適正性確保の観点からも、特定製品の採用については、その必要性を十分に吟味する必要がある。

なお、最終的な情報システム調達仕様書には、特定製品の内容について具体的に示す必要がある。

表－ 37　特定製品の採用有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	特定製品の指定がない	特定製品を特に利用しない場合に選択する。
レベル１	一部に特定製品の指定がある	調達対象の一部に、特定製品を利用する場合に選択する。 なお、特定製品としてオープンソースソフトを利用する場合には、一般にコストの低減が期待できるが、運用・保守も含め、対応可能性やコスト増加の可能性がないか、ベンダーに確認することが望ましい。
レベル２	サポートが困難な特定製品の指定がある	特に一般的に流通していない、その技術・ノウハウを持つ会社が限られるような特定製品を指定する場合に選択する。 コストの増加や調達の適正性確保の問題が発生する可能性があるため、製品の指定を行う必要があるかどうか、十分に留意する。

第３節 実現方法要求事項シート

実現方法要求事項シートの項目は、実現方法について規定する性格のものを収めており、特に RFI やベンダー等へのヒアリングを通じて決めることを想定している。したがって、以下に記載した内容を参考にした上で、ベンダーに確認しながら設定すること。

A.2.1.1 冗長化（サーバ機器）

サーバを複数の機器により構成し、サーバの故障等に対して備えるかどうかを選択する。複数にする機器を増やすほど、故障等に対して対応力が強くなるがその分コストも発生する。RTO（目標復旧時間）に対しても整合のとれた選択をする必要がある（IPA の「高回復性モデルシステム基盤導入ガイド」[10]等が参考になる）。

表－ 38 冗長化（サーバ機器）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	非冗長構成	サーバはいずれも冗長化しない場合に選択する。 サーバに故障等が発生した場合には、修理若しくは代替するサーバにより対応されるまでは情報システムは復旧できないため、復旧に時間がかかる。
レベル１	特定のサーバで冗長化	データベースサーバ等特定のサーバのみ冗長化する。当該サーバに故障等が発生した場合には、冗長化されたサーバに切り替えることですぐに復旧することができる。ただし、その分のコストが発生する。
レベル２	すべてのサーバで冗長化	情報システムを構成するすべてのサーバを冗長化する。いずれのサーバに故障等が発生した場合にも、冗長化されたサーバに切り替えることですぐに復旧することができる。ただし、その分のコストが発生する。

A.2.5.1 冗長化（ストレージ機器）

情報を記録するストレージ機器本体を複数の機器により構成し、ストレージ機器の故障等に対して備えるかどうかを選択する。複数にするストレージ機器を増やすほど、故障等に対して対応力が強くなるがその分コストも発生する。RTO（目標復旧時間）とも整合のとれた選択をする必要がある。

表－ 39 冗長化（ストレージ機器）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	非冗長構成	ストレージ機器はいずれも冗長化しない場合に選択する。 ストレージ機器に故障等が発生した場合には、修理若しくは代替するストレージ機器により対応されるまでは情報システムは復旧できないため、復旧に時間がかかる。

[10] IPA「高回復力システム基盤導入ガイド（概要編、計画編）を公開」＜http://www.ipa.go.jp/sec/softwareengineering/reports/20120508.html＞（最終アクセス平成 26 年 2 月 5 日）。

レベル	設定値	設定時の考え方や留意点
レベル１	特定の機器のみ冗長化	特定のストレージ機器のみ冗長化する。当該ストレージ機器に故障等が発生した場合には、冗長化されたストレージ機器に切り替えることですぐに復旧することができる。ただし、その分のコストが発生する。
レベル２	すべての機器を冗長化	情報システムを構成するすべてのストレージ機器を冗長化する。いずれのストレージ機器に故障等が発生した場合にも、冗長化されたストレージ機器に切り替えることですぐに復旧することができる。ただし、その分のコストが発生する。

A.2.5.3　冗長化（ストレージのディスク）

ストレージ機器ではなく、ストレージ機器に含まれるディスクを複数のディスクにより構成し、ディスクの故障等に対して備えるかどうかを選択する。複数にするディスクを増やすほど、故障等に対して対応力が強くなるが、その分コストも発生する。RTO（目標復旧時間）や RPO（目標復旧地点）とも整合のとれた選択をする必要がある。

表－ 40　冗長化（ストレージのディスク）に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	非冗長構成	ディスクはいずれも冗長化しない場合に選択する。 ディスクに故障等が発生した場合には、修理若しくは代替ディスクにより対応されるまでは情報システムは復旧できないため、復旧に時間がかかる。また、記録されたデータは、別途バックアップされていた時点のデータしか残されない。
レベル１	RAID5 による冗長化	RAID5 と呼ばれる手法でディスクを冗長化する。高速性やディスクの使用効率は高いが、構成しているディスクが同時に 2 台以上故障するとデータを復旧できなくなる。
レベル２	RAID1 による冗長化	RAID1 と呼ばれる手法でディスクを冗長化する。同じ内容データを複数のディスクに複製する。ディスクの使用効率は低いが、同一のデータを複数のディスクに書き込む方式であるため、いずれかの 1 台のディスクが正常であればデータは復旧できる。RAID5 と比較し、コストが高くなるケースが多い。

A.3.1.1　復旧方針

大規模災害の発生時に当該システムが利用できなくなった場合に備えて、どのような代替システムを、どこに用意するかを選択する。

レベルを上げるほど、耐災害性を高めることはできるが、コストが増加することにも留意が必要である。

表－ 41　復旧方針に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	復旧しない	災害時に備えた復旧対策を行わない場合に選択する。
レベル１	限定された構成で情報システムを再構築	代替システムを、当該システムより性能の低いサーバ等（冗長化を省いた構成にする等）で構成し、当該システムと同じ場所に、災害後に再構築する場合に選択する。 代替システム運用中は、縮退運転等を許容する必要がある。また、当該システムの設置場所が被災した場合、代替システムが使えない可能性が高い。 代替システムのコストは限定している分、当該システムのコストより少なくて済む。
レベル２	同一の構成で情報システムを再構築	代替システムを、当該システムと同一の構成で、当該システムと同じ場所に、災害後に再構築する場合に選択する。 代替システム運用中も、当該システムを運用しているのと同等の処理性能等を得ることができる。しかし、当該システムの設置場所が被災した場合、代替システムが使えない可能性が高い。 単に当該システムを構築する場合に比べて、情報システムでほぼ倍のコストが必要になる。
レベル３	限定された構成を DR サイトで構築	代替システムを、当該システムより性能の低いサーバ等（冗長化を省いた構成にする等）で、当該システムが設置する場所から距離が離れた場所に、事前に構築する場合に選択する。 代替システム運用中は、縮退運転等を許容する必要がある。当該システムの設置場所が被災しても、同時被災さえなければ、情報システムの運用ができる。 代替システムのコストは限定している分、当該システムのコストより少ないが、スペース確保等のコストが必要となる。 なお、データセンター等の庁舎外にサーバを設置する場合は、庁舎がＤＲサイトの位置づけとなる場合もある。
レベル４	同一の構成を DR サイトで構築	代替システムを、当該システムと同一の構成で、当該システムを設置する場所から距離が離れた場所に、事前に構築する場合に選択する。 代替システム運用中も、当該システムを運用しているのと同等の処理性能等を得ることができる。当該システムの設置場所が被災しても、同時被災さえなければ、情報システムの運用ができる。 単に当該システムを構築する場合に比べて情報システムで、ほぼ倍のコストが必要になることに加えて、スペース確保等のコストが必要となる。

A.3.2.2　保管方法（外部保管データ）

バックアップデータを、どのような方法で、どこ（情報システムの設置場所と同一の場所か遠隔地か）に保管するかを選択する。

表－42　保管方法に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	媒体による保管	媒体によりバックアップデータを保管する場合に選択する。最もコストを必要としないが、リアルタイムによるデータバックアップはできない。 また、保管場所をシステム設置場所と同一とした場合には、同時被災の恐れがある（媒体の場合の保管場所は、「A.3.2.1　保管分散度（外部保管データ）」で定める）。
レベル１	同一システム設置場所内の別ストレージへのバックアップ	システム設置場所と同一の場所に置かれた別のストレージにデータバックアップを行う場合に選択する。 リアルタイムにデータバックアップを取得できるが、情報システムと同時被災の恐れがある。
レベル２	DR サイトへのリモートバックアップ	システム設置場所とは別の場所に置かれた別のストレージにデータバックアップを行う場合に選択する。 リアルタイムにデータバックアップの取得が可能であり、また、同時被災の恐れがない。しかし、情報システム、スペース、回線等の費用が必要である。

C.1.2.3　データ復旧の対応範囲

データの損失等が発生したときに、どのような事象に対して対応する必要があるかを定める。レベル 2 を実現するには、コストが高額になる可能性が高く、もし選択する場合には、その必要性とともに、ベンダーに対して、実現可能性やコストについて十分な確認が必要である。

表－ 43　バックアップ利用範囲に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	バックアップを取得しない	バックアップデータを一切取得しない場合に選択する。
レベル１	障害発生時のデータ損失防止	定められた頻度により、データをバックアップし、障害が発生した場合に復旧できるようにする場合に選択する。 通常データバックアップと言った場合には、このことを指すことが多い。
レベル２	変更・削除したファイルの復旧	データに何らかの変更・削除が発生するタイミングごとにデータバックアップを取得し、その変更・削除した状態から変更・削除を加える前の状態に戻せるようにする場合に選択する。 ファイルサーバ以外のサーバでは、実現できないと考えてよい。

C.1.2.4　バックアップ自動化の範囲

バックアップ操作について、どれだけ自動化をするかについて定めるものである。自動化の範囲を広くするほど、作業負担は減るが、構築時のコストは大きくなる。

バックアップ作業をすべて委託する場合には、必ずしも定める必要はなく、ベンダーの提案に任せることでよい項目である。

表－ 44　バックアップ自動化の範囲に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	全ステップを手動で行う	バックアップ操作について、すべて手動で行う場合に選択する。
レベル１	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンドの入力）	バックアップ操作について、外部媒体の交換や開始の操作等は手動で行うが、他の作業は自動で実施する場合に選択する。 どのデータをバックアップするか等の制御の仕組みが必要となる。
レベル２	1 ステップのみ手動で行う（外部媒体交換のみ）	バックアップ操作について、外部媒体の交換のみ手動で実施し、他の作業は自動で実施する場合に選択する。 どのデータをバックアップするか等の制御の仕組みとともに、スケジュール管理やバックアップ作業をしてよいかどうかを判断するための監視制御の仕組みが必要となる。
レベル３	全ステップを自動で行う	バックアップ操作について、すべて自動で実施する場合に選択する。 レベル 2 に加えて、バックアップデータを保存する媒体を物理的に制御する仕組みが必要になる。

C.1.3.1　監視情報

監視を行う情報の深さについて定める。深くすればするほど、監視のレベルは上がるが、システム面や体制面のコストが必要になる。

表－ 45　監視情報に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	監視を行わない	監視を特に行わない場合に選択する。
レベル１	死活監視を行う	情報システムや情報システムを構成するソフトウェアや機器等が動作しているかどうかの監視を行う場合に選択する。 障害の発生の有無を把握することができる。
レベル２	エラー監視を行う	レベル 1 に加え、情報システムにおいて、エラーが発生しているかどうかの監視を行う場合に選択する。 情報システムの障害だけでなく、異常動作を把握することができる。
レベル３	エラー監視（トレース情報を含む）を行う	レベル 2 に加え、情報システムにおいて、エラーが発生しているかどうかの監視を行い、そのエラーの内容についての詳細情報も監視を行う場合に選択する。 異常動作の把握とともに、その原因を検証することが可能になる。
レベル４	リソース監視を行う	レベル 3 に加え、情報システムのリソース（CPU の処理量やメモリの使用量、ディスク容量、ネットワーク使用帯域等）について監視を行う場合に選択する。 情報システムのリソースの使用状況を把握することができ、障害の予防や性能維持のための検討の判断材料を得ることができる。

レベル	設定値	設定時の考え方や留意点
レベル５	パフォーマンス監視を行う	レベル４に加え、情報システムの処理能力（応答時間や処理量等）について監視する場合に選択する。 処理能力の低下等の状況を把握することができ、障害の予防や性能維持のための検討の判断材料を得ることができる。

C.4.2.1　試験用環境の設置有無

情報システムに何らかの手を加えた際に、情報システムが正常に動作するかどうかを検証するための試験用環境を設置するかどうかを定めるものである。法制度改正が多いなど、情報システムに頻繁に手が加えられる情報システムの場合には、試験用環境の整備が望まれる。

なお、近年の仮想化技術の進展により、仮想化技術を導入した情報システムの場合には、比較的コストをかけずに試験用環境を用意できるようになっている。

表－ 46　試験用環境の設置有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	情報システムの試験用環境を設置しない	情報システムの試験用環境を設置しない場合に選択する。 その分のコストは不要だが、万が一不具合が発生した場合には、業務に直接影響が出る恐れがある。
レベル１	情報システムの開発用環境と併用する	情報システムの試験用環境を情報システムの開発用環境と兼ねる場合に選択する。 独立した環境を用意しなくてもよい分コストがかからなくて済むが、本番環境と試験用環境に異なる点がないかの管理や、試験作業と開発作業の調整が必要となる。
レベル２	専用の試験用環境を設置する	情報システムの専用の試験用環境を用意する場合に選択する。 試験用環境について管理がしやすいが、専用の環境を用意する分のコストが必要となる。

C.6.2.1　問い合わせ対応窓口の設置有無

情報システムの問い合わせ対応のサポート窓口として、どのようなサービスを利用するかを定める。

表－ 47　問い合わせ対応窓口の設置有無に関するレベル設定時の考え方や留意点

レベル	設定値	設定時の考え方や留意点
レベル０	問い合わせ対応窓口の設置について規定しない	問い合わせ対応窓口を特に求めない場合に選択する。
レベル１	ベンダーの既設コールセンターを利用する	情報システム（機器やソフトウェア等）についての一般利用者対象の問い合わせ窓口を利用したサポートを受ける場合に選択する。

レベル	設定値	設定時の考え方や留意点
レベル２	ベンダーの常駐等専用窓口を設ける	発注者専用の情報システムに関する問い合わせ対応窓口を設置する場合に選択する。 発注者の事情に応じた問い合わせに即応できるが、専用窓口を設ける分の人件費等が必要となるため、必要なコストは多くなる。

用語集

● 日本語

No	用語	説明
1	AP サーバ	アプリケーションを搭載しているサーバ。
2	DB サーバ	データベースを搭載しているサーバ。
3	DoS 攻撃	第三者のコンピュータに攻撃プログラムを仕掛けて踏み台にし、その踏み台としたコンピュータから標的とするコンピュータに大量のパケットを同時に送信する攻撃。
4	DDoS 攻撃	第三者のコンピュータに攻撃プログラムを仕掛けて踏み台にし、その踏み台とした複数台のコンピュータから標的とするコンピュータに大量のパケット送信する攻撃。
5	DR サイト	災害対策として遠隔地に設置している代替システム。
6	RoHS 指令	通信機器に有害な化学物質の使用を禁止する指令。
7	Web アプリケーション	Web 技術を用いて設計、構築されたアプリケーションソフト。
8	Web サーバ	Web 技術を用いて、利用者に情報を送信するサーバ。
あ行		
9	アーカイブ	重要情報等を長期間保存・記録すること。
10	アクセス	ネットワークを経由して他のコンピュータと接続すること。(接続ケーブル等により) 物理的に接続するという意味ではなく、コンピュータ間でのデータの転送のことを指す。
11	アップデート	情報システムを構成するソフトウェアの小規模な更新、改善、修正、機能追加などの行為。
12	インターフェース	機器、情報システム、人等の接点において、互いに情報や信号をやりとりするための手順や規約、規格を定めたもの。機器間でいえばコネクタの形状や電気信号の形式、情報システム間であればプログラム間でデータをやり取りする手順や形式、人と情報システムの間であれば、情報を表示・入力する方法や形式を指す。
13	ウィルス定義ファイル	コンピュータウィルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイル。アンチウィルスソフト(ワクチンソフト)がコンピュータウィルスやワームを検出するのに利用される。
14	オープンソース	ソースコードをインターネットなどを通じて無償で公開し、誰でもそのソフトウェアの改良、再配布が行えるようにする行為。また、そのようなソフトウェア。
15	オペレーション	情報システムの操作方法。
16	オンサイト	オンサイトサービスの略称。出張修理サービスのことで、メーカーや販売店が直接出向いて行う情報システム等の修理や保守を実施してくれるサービス。
17	オンラインリクエスト件数	情報システムに対するネットワークを経由した接続要求件数。

No	用語	説明
か行		
18	可用性	正当な権限を持った利用者が要求した際は、必要なときにいつでも情報システムを利用できること。
19	完全性	情報システムが故意・過失・災害などで改ざんされたり、破壊されたりしないようにすること。
20	機密性	正当な権限を持った利用者だけが情報に触れることができる状態。また、そのような状態を確保・維持すること。
21	クライアント	クライアントコンピュータの略。接続されているサーバの処理機能を利用する端末。
22	クラウド	クラウドコンピューティングの略。ソフトウェアやデータを、インターネット等のネットワークを通じてサービスの形で必要に応じて利用する情報システムの形態。
23	クラスタ	複数台のコンピュータ（サーバ等）を連結させ処理を実行すること。
24	コマンド	利用者が情報システムへの入力機器を用いて処理を命令すること。
さ行		
25	差分バックアップ	利用する情報システムのデータをバックアップする際、前回のバックアップ以降に追加・更新された部分だけをバックアップする行為。
26	縮退運転	何らかの事態が発生した場合、機能を縮小して処理を実施する行為。
27	冗長化	機器等を多重構成にして設置する等により、一部の機器等が故障してもサービスを継続して提供できるようにすること。
28	ジョブ起動	情報システム処理の開始のこと。
29	スクリプト	特定の言語の表記に使う、ひとまとまりの文字の体系。
30	ストレージ	データやプログラムを記憶する装置。
31	セキュアコーディング	脆弱性のない、安全なソフトウェアプログラミング手法。
32	センドバック	センドバックサービスの略称。異常や故障が発生した製品をユーザがメーカー側に直接送付すると、メーカー側で修理・動作確認後返却してくれるサービス。
33	ソースコード	プログラミング言語を用いて記述したコンピュータプログラム。
た行		
34	ターンアラウンドタイム	利用する情報システムに接続してから、処理結果の出力が終了するまでの経過時間。
35	耐タンパデバイス	物理的、あるいは論理的に内部の情報を読み取られることに対する耐性をもった装置。
36	ディスクアレイ	複数のハードディスクを束ねて 1 台のハードディスクのように利用する装置。
37	データセンター	耐震性を備えた強固な建築物で顧客のサーバを預かり、インターネットへの接続回線や保守・運用サービスなどを提供する施設。
38	テーブル	データの要素を縦横に格子状に配置したもの。
39	デフラグ	データの断片化を解消し、空き容量を増加させる技術。

No	用語	説明
は行		
40	バージョンアップ	情報システムを構成する、ソフトウェアやハードウェアを新しいバージョンにすること。また、機能の向上や不具合の修正などの改良や改善がされる行為。
41	パケット	ネットワークの通信時、送信先のアドレス等の制御情報を付加されたデータの小さなまとまり。
42	パッチ	修正を行うために変更点(差分情報)のみを抜き出して列挙したファイル。
43	ピーク時	利用する情報システムへの負荷が最大値になった状態。
44	ピークモデル	ユーザのシステム利用による負荷集中が最大になる地点にいたる経過を想定したもの。
45	ファイアーウォール	情報システムへのネットワークを介した外部侵入を防ぐ機器。
46	踏み台攻撃	セキュリティ対策の脆弱なサイトに不正侵入し、他サイトの攻撃の中継サイトとして利用すること。
47	ベンダー	情報システムの製品を供給する事業者。情報システムを構築、運用する事業者を含む。
48	ポート	外部とデータを入力するための、パソコン、サーバ等機器の LAN 接続末端部分。
49	ボット	不正プログラムの一種で自動化された処理を行うプログラムの総称。
ま行		
50	マルウェア	コンピュータウィルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェアの総称。
51	ミドルウェア	OS と業務アプリケーションの中間で処理を補完するソフトウェア。
52	文字コード	文字や記号をコンピュータで扱うために、文字や記号一つ一つに割り当てられた固有のコード。
ら行		
53	ライフサイクル	情報システムが構築されてから、運用を終了するまでの過程をモデル化したものであり、一般的には計画，分析，設計，製造，テスト，運用，保守の工程を指す。
54	リカバリ	情報システムやデータ等を復旧させる行為。
55	リクエスト件数	利用する情報システムに対して接続した件数。
56	リモートオペレーション	情報システムの設置環境より離れた環境からネットワークを介した監視や操作を実施する行為。
57	リモート監視	情報システムの設置環境より離れた環境からネットワークを介して監視を実施する行為。
58	リモート操作	情報システムの設置環境より離れた環境からネットワークを介して情報システムを操作する行為。
59	リモートバックアップ	情報システムの設置環境より離れた環境でネットワークを介してバックアップを実施する行為、又は設備。
60	リモート保守	情報システムの設置環境より離れた環境からネットワークを介して保守を実施する方法。
61	レスポンス	ネットワークを経由して接続した情報システムからの応答行為。
62	レスポンスタイム	ネットワークを経由して接続した情報システムからの応答があるまでの経過時間。
63	ログ	システム利用状況やデータ通信の記録

No	用語	説明
64	ログローテート	ログファイルのサイズが大きくなりすぎないように、定期的に古いファイルを上書きすること。
わ行		
65	ワーム	不正プログラムの一種で単独で動作する悪意あるプログラムを指す。

●アルファベット

No	用語	説明
1	IPS	Intrusion Prevention System の略称。サーバやネットワークへの不正侵入を阻止するツール。ネットワークの境界などに設置する専用の機器や、サーバに導入するソフトウェアなどの形態がある。
2	LAN	Local Area Network の略称。ケーブルや無線などを使って、同じ建物の中にあるサーバや通信機器、プリンタなどを接続し、データをやり取りするネットワーク。
3	RAID	Redundant Arrays of Inexpensive Disks の略称。複数のハードディスク等の外部記録装置を一台の装置のように管理する技術。複数の装置にデータを分散して記録することにより、高速化や耐障害性の向上を図ることができる。記録の方式により複数の種類がある。
4	RLO（目標復旧レベル）	Recovery Level Objective の略称。業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（情報システムの復旧・特定業務・すべての業務）の目標値。
5	RPO（目標復旧地点）	Recovery Point Objective の略称。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情報システムをどの時点まで復旧するかを定める目標値。
6	RTO（目標復旧時間）	Recovery Time Objective の略称。業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。
7	SLA	Service Level Agreement の略称。サービスの品質に対する利用者側の要求水準と提供者側の運営ルールについて明文化したもの。
8	UL60950	情報機器の製品安全規格の一種。
9	WAF	Web Application Firewall の略。Web アプリケーション上の脆弱性をカバーする装置。

参考資料　IPA の非機能要求グレードとの関係

「非機能要求グレード（地方公共団体版)」は、地方公共団体が情報システム調達仕様書を検討する際に利用することを目的に、IPA が作成した「非機能要求グレード」（2013 年 4 月）を基に地方公共団体の業務やその情報システムの特性に合わせて一部変更を行っている。

IPA の非機能要求グレードと非機能要求グレード（地方公共団体版）の成果物との対応関係と主な変更の内容は下表に示すとおりである。

表－ 48　IPA の非機能要求グレードと地方公共団体版の成果物との対応

IPA の非機能要求グレード		地方公共団体版
①　利用ガイド（解説編）	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したもの。	「調査研究報告書」が相当。 ・主に IPA の非機能要求グレードを基にどのような考えで地方公共団体版を作成したかについて示している。
②　利用ガイド（利用編）	非機能要求グレードの具体的な利用方法について解説したもの。	本「利用ガイド」が相当。 ・情報システム調達仕様書の作成を目的とした利用方法を示している。
③　グレード表	３つのモデルシステムと重要な非機能要求項目に対する要求レベルとグレードを一覧表化したもの。	「活用シート」に集約。 ・モデルシステムは、４つの業務・情報システムのグループに変更。
④　項目一覧	システム基盤に関わる非機能要求項目を発注者／受注者間で漏れなく共通に認識できるよう体系化した一覧表。	「活用シート」に集約。
⑤　樹系図	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。	「項目一覧」が相当。
⑥　活用シート	グレード表と項目一覧の内容をまとめた一覧表。スプレッドシート形式で、使用条件の範囲で変更が可能。	「活用シート」が相当。 ・全 236 項目から、地方公共団体が情報システムを調達するために必要な 89 項目に集約（一部項目追加も実施)。 ・項番（例：A.1.1.1）については、元の番号を引き継いでいるが、追加した項目や概念を変更した項目については新たな番号を付与している。 ・地方公共団体の実状に合わせて、用語表現等を調整している。 ・情報システム調達仕様書の作成を目的に、シート構成や各シートの項目についても追加や順番の変更等をしている。

非機能要求グレード活用シート
（地方公共団体版）
項目一覧

平成26年3月

財団法人　地方自治情報センター

[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及び財団法人地方自治情報センターが保有しています。

2. 本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものです。

3. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。詳細は、「利用ガイド」の「第3章　第8節 検討結果の情報システム調達仕様書への反映」をご参照ください。

4. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、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及び財団法人地方自治情報センターは、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又は財団法人地方自治情報センター又は第三者の著作権、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及び財団法人地方自治情報センターは、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、財団法人地方自治情報センターまでご連絡下さい。

非機能要求グレード（地方公共団体版） 項目一覧

・本シートは、非機能要件グレード（地方公共団体版）の項目を一覧化したものである。加工して、RFIの回答シートや各団体の作業用に活用することを想定している。

大項目	中項目	項番	メトリクス（指標）	掲載シート
可用性	継続性	A.1.3.1	RPO（目標復旧地点）（業務停止時）	Ⅱ
		A.1.3.2	RTO（目標復旧時間）（業務停止時）	Ⅱ
		A.1.3.3	RLO（目標復旧レベル）（業務停止時）	Ⅱ
		A.1.4.1	システム再開目標（大規模災害時）	Ⅱ
		A.1.5.1	稼働率	Ⅱ
	耐障害性	A.2.1.1	冗長化（サーバ機器）	Ⅲ
		A.2.5.1	冗長化（ストレージ機器）	Ⅲ
		A.2.5.3	冗長化（ストレージのディスク）	Ⅲ
	災害対策	A.3.1.1	復旧方針	Ⅲ
		A.3.2.1	保管場所分散度（外部保管データ）	Ⅲ
		A.3.2.2	保管方法（外部保管データ）	Ⅲ
性能・拡張性	業務処理量	B.1.1.1	ユーザ数	Ⅱ
		B.1.1.2	同時アクセス数	Ⅱ
		B.1.1.3	データ量（項目・件数）	Ⅱ
		B.1.1.4	オンラインリクエスト件数	Ⅱ
		B.1.1.5	バッチ処理件数	Ⅱ
		B.1.2.1	ユーザ数増大率	Ⅱ
		B.1.2.2	同時アクセス数増大率	Ⅱ
		B.1.2.3	データ量増大率	Ⅱ
		B.1.2.4	オンラインリクエスト件数増大率	Ⅱ
		B.1.2.5	バッチ処理件数増大率	Ⅱ
		B.1.3.1	保管期間（データ）	Ⅲ
	性能目標値	B.2.1.4	通常時オンラインレスポンスタイム	Ⅱ
		B.2.1.5	アクセス集中時のオンラインレスポンスタイム	Ⅱ
		B.2.2.1	通常時バッチレスポンス順守度合い	Ⅱ
		B.2.2.2	アクセス集中時のバッチレスポンス順守度合い	Ⅱ
運用・保守性	通常運用	C.1.1.1	運用時間（平日）	Ⅱ
		C.1.1.2	運用時間（休日等）	Ⅱ
		C.1.2.2	外部データの利用可否	Ⅰ
		C.1.2.3	データ復旧の対応範囲	Ⅲ
		C.1.2.4	バックアップ自動化の範囲	Ⅲ
		C.1.2.5	バックアップ取得間隔	Ⅱ
		C.1.3.1	監視情報	Ⅲ
	保守運用	C.2.3.5	OS等パッチ適用タイミング	Ⅰ
	障害時運用	C.3.3.1	対応可能時間	Ⅱ
		C.3.3.2	駆けつけ到着時間	Ⅱ
		C.3.3.3	障害検知通知時間	Ⅱ
	運用環境	C.4.1.1	開発用環境の設置有無	Ⅲ
		C.4.2.1	試験用環境の設置有無	Ⅲ
		C.4.3.1	マニュアル準備レベル	Ⅱ
	リモートオペレーション	C.4.4.1	リモート監視地点	Ⅰ
		C.4.4.3	リモート操作時の接続方法	Ⅰ
	運用環境	C.4.5.1	外部システムとの接続有無	Ⅱ
	サポート体制	C.5.1.2	保守契約（ハードウェア）の範囲	Ⅱ
		C.5.2.2	保守契約（ソフトウェア）の範囲	Ⅱ
		C.5.3.1	ライフサイクル期間	Ⅱ
		C.5.5.1	一次対応役割分担	Ⅱ
		C.5.6.2	ベンダー側対応時間帯	Ⅱ
		C.5.9.1	定期報告会実施頻度	Ⅲ
		C.5.9.2	報告内容のレベル	Ⅲ
	その他の運用管理方針	C.6.2.1	問い合わせ対応窓口の設置有無	Ⅲ

Copyright ©2010-2014 IPA,LASDEC

非機能要求グレード（地方公共団体版） 項目一覧

移行性	移行時期	D.1.1.1	システム移行期間	Ⅲ
		D.1.1.2	システム停止可能日時	Ⅱ
		D.1.1.3	並行稼働の有無	Ⅲ
	移行対象（機器）	D.3.1.1	設備・機器の移行内容	Ⅱ
	移行対象（データ）	D.4.1.1	移行データ量	Ⅱ
	移行計画	D.5.1.1	移行のユーザ/ベンダー作業分担	Ⅱ
セキュリティ	前提条件・制約条件	E.1.1.1	順守すべき規程、ルール、法令、ガイドライン等の有無	Ⅰ
	セキュリティリスク分析	E.2.1.1	リスク分析範囲	Ⅰ
	セキュリティ診断	E.3.1.2	Web診断実施の有無	Ⅲ
	セキュリティリスク管理	E.4.3.4	ウィルス定義ファイル適用タイミング	Ⅰ
	アクセス※・利用制限	E.5.1.1	管理権限を持つ主体の認証	Ⅰ
		E.5.2.1	システム上の対策における操作制限度	Ⅰ
	データの秘匿	E.6.1.1	伝送データの暗号化の有無	Ⅰ
		E.6.1.2	蓄積データの暗号化の有無	Ⅰ
	不正追跡・監視	E.7.1.1	ログの取得	Ⅰ
		E.7.1.3	不正監視対象（装置）	Ⅰ
	Web対策	E.10.1.1	セキュアコーディング、Webサーバの設定等による対策の強化	Ⅰ
		E.10.1.2	WAFの導入の有無	Ⅰ
システム環境・エコロジー	システム制約/前提条件	F.1.1.1	構築時の制約条件	Ⅱ
		F.1.2.1	運用時の制約条件	Ⅱ
	システム特性	F.2.2.1	クライアント数	Ⅱ
		F.2.5.1	特定製品の採用有無	Ⅱ
	適合規格	F.3.1.1	規格取得の有無(安全性)	Ⅰ
		F.3.2.1	規格取得の有無（有害物質）	Ⅰ
	環境マネージメント	F.5.1.1	グリーン購入法対応度	Ⅰ

Copyright ©2010-2014 IPA,LASDEC

非機能要求グレード活用シート
（地方公共団体版）

平成26年3月

財団法人　地方自治情報センター

非機能要求グレード活用シート
（地方公共団体版）

業務・情報システムグループ①

平成26年3月

財団法人　地方自治情報センター

[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及び財団法人地方自治情報センターが保有しています。

2. 本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものです。

3. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。詳細は、「利用ガイド」の「第3章　第8節 検討結果の情報システム調達仕様書への反映」をご参照ください。

4. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、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及び財団法人地方自治情報センターは、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又は財団法人地方自治情報センター又は第三者の著作権、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及び財団法人地方自治情報センターは、本資料のシステム開発への利用、開発された情報システムの使用、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、財団法人地方自治情報センターまでご連絡下さい。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○			2 外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、本情報システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				
C.2.3.5		保守運用	OS等パッチ※4適用タイミング	OS等パッチ※情報の展開とパッチ※適用のポリシー※に関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。	○	○	P29	4 緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチ※を適用しない	障害発生時にパッチ※適用を行う	定期保守時にパッチ※適用を行う	緊急性の高いパッチ※のみ即時に適用を行う	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチ※がリリースされるたびに適用を行う	【注意事項】 リリースされるパッチ※の種類（個別パッチ※／集合パッチ※）よって選択レベルが変わる場合がある。 セキュリティパッチ※については、セキュリティの項目でも検討すること（E.4.3.3）。
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	−		P30	1 庁内LANを介してリモート監視を行う	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [−] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。	−		P30	0 リモート操作※を行わない	ベンダーによるリモート操作はセキュリティの観点から実施を禁止していることを想定。 [+]サーバ等が複数拠点に分散する場合、または、設置場所がベンダーのサポート拠点から遠方にある場合	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				【注意事項】 リモート操作を実施できる範囲は、あらかじめ協議し決定しておく必要がある。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク など	○	○		1 有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り						【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、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。
E.2.1.1		セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクル※の確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [−] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	○	P30	2 定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。	○		P31	1 1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。
E.5.2.1			システム上の対策における操作制限度	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例）コマンド実行制,ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○			1 必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可					
E.6.1.1		データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。	○		P31	1 認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。
E.6.1.2			蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○		P32	1 認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化				【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.7.1.1		不正追跡・監視	ログ※の取得	不正を検知するために、監視のための記録（ログ※）を取得するかどうかの項目。 なお、どのようなログ※を取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログ※を取得する場合には、不正監視対象と併せて、取得したログ※のうち、確認する範囲を定める必要がある。	○			1 必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログ※は、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等
E.7.1.3			不正監視対象（装置）	サーバ、ストレージ※等への不正アクセス※等の監視のために、ログ※を取得する範囲を確認する。 不正行為を検知するために実施する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	Webアプリケーション※特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング※、Webサーバ※の設定等による対策の実施を検討する必要がある。	○		P32	1 対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [−] Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					【注意事項】 また、実施した結果の有効性を確認するための専門家のレビューやソースコード※診断、ツールによるチェック等についても検討する必要がある。 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。 Webシステムで考慮すべき項目。
E.10.1.2			WAF※の導入の有無	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。	○		P33	0 無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 Webシステムで考慮すべき項目。
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。	−		P33	1 規格取得の必要有り	機器の規格取得に関して指定があった場合を想定。 [−] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り					
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	△		P34	1 RoHS指令※相当取得	RoHS指令※対応の装置が指定された場合を想定。 [−] 特に指定が無かった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得					
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	−		P34	0 対処不要	団体の方針によるものと想定。 [+]団体の方針による。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※4（業務停止時）	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情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	3	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [－] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P35	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [－] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P36	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [－] 影響を切り離せる機能がある場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）
A.1.4.1			システム再開目標（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	○	P37	4	3日以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1			稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	○	○	P38	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [－]地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [－] 特定のユーザのみ使用することを合意できた場合	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				
B.1.1.2			同時アクセス数	同時アクセス※数とは、ある時点で情報システムにアクセス※しているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			1	同時アクセス※の上限が決まっている	情報システムに対してどのようなピークモデル※を想定しているか確認する。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセス※のみ	同時アクセス※の上限が決まっている	不特定多数のアクセス※有り				
B.1.1.3			データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○			0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ量が明確である	主要なデータ量のみが明確である					【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民基本台帳システムであれば住民データ・世帯データ・異動データ等がある。
B.1.1.4			オンラインリクエスト件数※	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数※が明確である	主な処理のリクエスト件数※のみが明確である					【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理などがある。
B.1.1.5			バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	-	*	0	1	2	3	4	5	
B.1.2.1			ユーザ数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とユーザ数が最大になる時点のユーザ数の倍率。	△			1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [-] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.2			同時アクセス※数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点と同時アクセス数が最大になる時点の同時アクセス数の倍率。	△			1	1.2倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [-] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加が相関関係でない場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.3			データ量増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とデータ量が最大になる時点のデータ量の倍率。	△			1	1.2倍	業務の手順によって情報システムで扱うデータ量がどの程度増加するかを確認する。 [-] データを蓄積しないゲートウェイシステムの場合 [+] 過去のデータを長期間保存する情報システムの場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.4			オンラインリクエスト件数※増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とオンラインリクエスト件数が最大になる時点のオンラインリクエスト件の倍率。	△			1	1.2倍	情報システムの制約となるリクエスト数※の見通しを確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 オンラインリクエスト件数※は単位時間（1時間当たりの件数等）を明らかにして確認する。
B.1.2.5			バッチ処理件数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とバッチ処理件数が最大になる時点のバッチ処理件数の倍率。	△			1	1.2倍	情報システムの制約となる処理件数を確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 バッチ処理件数は単位時間（1日当たりの件数等）を明らかにして確認する。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	オンラインシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス※が必要かについて確認する。アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス※集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	○	P39	3	3秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※		○	○	P40	2	5秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.2.1			通常時バッチレスポンス※順守度合い	バッチシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム※）が必要かについて確認する。更に、アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時※・縮退運転※時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○	○		2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い		○	○		2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時※のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時※に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [-] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	-	*	0	1	2	3	4	5	
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	1	定時内での利用（1日8時間程度利用）	主に、開庁時間内での利用を想定 [–] 不定期に利用するシステムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。
C.1.1.2			運用時間（休日等）	土日/祝祭日や年末年始に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			
C.1.2.5			バックアップ取得間隔	バックアップ取得間隔	○		P41	4	日次で取得	全体バックアップは週次で取得する。しかし、RPO※要件である、1日前の状態に戻すためには、毎日差分バックアップ※を取得しなければならないことを想定。 [–] RPO※の要件が[–]される場合 [+] RPO※の要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	
C.3.3.1		障害時運用	対応可能時間	情報システムの異常検知時に保守員が作業対応を行う時間帯。	–			0	ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	ベンダーの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う				
C.3.3.2			駆けつけ到着時間	情報システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	–	○	P42	4	保守員到着が異常検知から数時間内	[+]対応が必要な場合 [–]地理的条件・コスト等により、制限が有る場合。	仕様の対象としない	ベンダーによる提案事項	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	
C.3.3.4			障害検知通知時間	障害の発生を検知した場合に、利用者（システム運用担当者）に通知するまでの時間。		○	P42	0	障害を検知しない	本項目は、常駐保守または、サーバをデーターセンター※に設置した場合。 [+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	障害を検知しない	24時間以内	8時間以内	3時間以内	1時間以内	30分以内	
C.4.3.1		運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○			2	情報システムの通常運用と保守運用のマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ※作業手順などを示した保守マニュアルも作成する。 [–] 保守作業はすべてベンダーに依頼するため、通常運用に必要なオペレーション※のみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ※収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。
C.4.5.1			外部システムとの接続有無	情報システムの運用に影響する外部システムとの接続の有無に関する項目。	○			1	庁内の外部システムと接続する	庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [–] データのやり取りを行う多システムが存在しない場合 [+] 庁外のシステムに接続して、データのやり取りを行う場合	仕様の対象としない	ベンダーによる提案事項	外部システムと接続しない	庁内の外部システムと接続する	庁外の外部システムと接続する				【注意事項】 接続する場合には、そのインターフェース※（接続ネットワーク・通信方式・データ形式等）について確認すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	保守が必要な対象ハードウェアに対する保守契約の種類。	－		P43	4	定額保守（オンサイト※）	オンサイト※の定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	随時保守（センドバック※）	定額保守（センドバック※）	随時保守（オンサイト※）	定額保守（オンサイト※）		
C.5.2.2			保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○			2	アップデート※	ソフトウェアが法改正等によりバージョンアップ※した場合に、アップデートする権利を含めることを想定。 [－] アップデート※権を必要としない場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート※				【注意事項】 アップデート権の範囲については、事前にベンダーと協議しておくこと。 ライフサイクル期間中に、OSやミドルウェアのバージョンアップが必要となる場合は、バージョンアップ後の情報システムの動作保障等についてあらかじめベンダーと協議しておくこと。 インターネットに公開する外部システムの場合は、最新ブラウザへの対応等についてもあらかじめベンダーと協議しておくこと。
C.5.3.1			ライフサイクル期間	運用保守の対応期間及び、実際に情報システムが稼動するライフサイクルの期間。ライフサイクルとは情報システムの利用期間（次回のシステム更改までの期間）のことを示している。	△		P44	1	5年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	仕様の対象としない	ベンダーによる提案事項	3年	5年	7年				【注意事項】 製品の保守可能期間よりも長い期間のライフサイクル※となる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。 【注意事項】 アプリケーションのパッケージソフトのライフサイクル※とは異なるので注意が必要。 通常のサポート期間は5年程度であり、それ以上の期間を求める場合には、コストの上昇を招くか、対応可能なベンダーが非常に限られるおそれがあるので注意が必要。 クラウド※の場合は、サービス提供可能期間として捉える。 【注意事項】 ライフサイクル期間中は、ソフトウェア・ハードウェアのサポート切れが発生しないようにする必要が有る。 クライアントPCとして、情報システム専用でない（例えば庁内LAN用に一括購入した）PCを使用する場合等は、更改時のOSバージョンアップ等についてあらかじめベンダーと協議しておくこと。
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダーの役割分担。	－			2	すべてベンダーが実施	[－]ユーザにて一次切り分けが実施できるスキルが有る場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザが実施	一部ユーザが実施	すべてベンダーが実施				
C.5.6.2			ベンダー側対応時間帯	一次対応のベンダーの対応時間。	－			1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [－]保守契約をしない場合	仕様の対象としない	ベンダーによる提案事項	対応無し	ベンダーの定時時間内（9～17時）	ユーザの指定する時間帯	24時間対応			
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	○			4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [－] 停止を増やす場合	仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。 レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○		P44	3	移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。 [－] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェア※を入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。	○		P45	2	10TB未満	10TB（テラバイト）未満のデータを移行する必要がある。 [－] 1TB未満の場合 [+] 10TB以上の場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上			
D.5.1.1		移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。	○			1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など	○			1 制約有り（重要な制約のみ適用）	庁内規約などが存在する場合を想定。 [−] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1			運用時の制約条件	運用時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク ・リモートからの運用の可否 など	○			1 制約有り（重要な制約のみ適用）	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				
F.2.2.1		システム特性	クライアント※数	情報システムで使用され、管理しなければいけないクライアント※（端末）の数。 専用端末、共用端末問わず、当該システムで使用するクライアント数を示す。	△			1 上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合	仕様の対象としない	ベンダーによる提案事項	特定クライアント※のみ	上限が決まっている	不特定多数のクライアント※が利用				
F.2.5.1		システム特性	特定製品の採用有無	ユーザの指定によるオープンソース※製品や第三者製品(独立系ソフトウェア会社/独立系ハードウェア会社)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。	―		P45	1 一部に特定製品の指定がある	構成する機器に関して固有の製品が指定された場合を想定。 [−] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　ー：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。
2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目
3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ
4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①			レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
A.2.1.1	可用性	耐障害性	冗長化※4（サーバ機器）	サーバ機器を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	2	すべてのサーバで冗長化※	すべてのサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長※構成	特定のサーバで冗長化※	すべてのサーバで冗長化※				【レベル1】 特定のサーバで冗長化※とは、情報システムを構成するサーバの種別（DBサーバ※やAPサーバ※、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化※を指定する場合もある。
A.2.5.1			冗長化（ストレージ※機器）	ディスクアレイ※などの外部記憶装置を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	2	すべての機器を冗長化※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	特定の機器のみ冗長化※	すべての機器を冗長化※				【レベル1】 特定の機器のみとは、導入するストレージ※装置に格納するデータの重要度に応じて、耐障害性の要求が装置ごとに異なる場合を想定している。
A.2.5.3			冗長化（ストレージ※のディスク）	ハードディスクを物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P48	1	RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	RAID5※による冗長化※	RAID1※による冗長化※				【レベル2】 性能での要件からRAID0※との組み合わせを検討する。
A.3.1.1		災害対策	復旧方針	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための代替の機器として、どこに何が必要かを決める。	○		P48	3	限定された構成をDRサイト※で構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイト※で構築	同一の構成をDRサイト※で構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化※の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。
A.3.2.1			保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管する。	○			2	1ヶ所（遠隔地）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（遠隔地）			【注意事項】 ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。
A.3.2.2			保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するための方法。	○		P49	2	DRサイト※へのリモートバックアップ※	遠隔地にリモートバックアップすることを推奨する。 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	媒体による保管	同一システム設置場所内の別ストレージ※へのバックアップ	DRサイト※へのリモートバックアップ※				
B.1.3.1	性能・拡張性	業務処理量	保管期間（データ）	情報システムが参照するデータのうち、OSやミドルウェア※のログ※などのシステム基盤が利用するデータに対する保管が必要な期間。必要に応じて、データの種別ごとに定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	△			3	5年	税制などの対応で保管期間が規定されているという想定。 [−] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	仕様の対象としない	ベンダーによる提案事項	6ヶ月	1年	3年	5年	7年	10年以上有期	【レベル】 それぞれの情報システム（住民情報、税等）でデータの保管期間が異なる場合は、それぞれの対象データについて決めること。
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのような事象に対して対応する必要があるかを示す項目。	○		P50	1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	変更・削除したファイルの復旧				【注意事項】 職員の入力ミスを想定した変更・削除したファイルの復旧の場合、情報システムとしては正常に完了してしまった処理を元に戻さなければならないため、ファイルサーバ以外の情報システムでは実現できないと考えて良い。
C.1.2.4			バックアップ自動化の範囲	バックアップ自動化の範囲。 バックアップ運用には、 ・スケジュールに基づくジョブ起動※ ・バックアップ対象の選択 ・バックアップ先メディアの選択（外部媒体交換） ・ファイル転送 などといった作業ステップが存在する。別地保管を媒体搬送で行う場合の、外部媒体交換はここには含まない。	−		P50	2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	仕様の対象としない	ベンダーによる提案事項	全ステップを手動で行う	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンド※の入力）	1ステップのみ手動で行う（外部媒体交換のみ）	全ステップを自動で行う			

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ①			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
C.1.3.1			監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	○		P51	3	エラー監視（トレース情報を含む）を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [－] 障害時は管理者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] エラー情報だけでなく、リソース使用状況も監視して、障害発生を未然に防ぎたい場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータス※がオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報※を含む場合は、どのモジュール※でエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループット※について判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。
C.4.1.1		運用環境	開発用環境の設置有無	開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。 本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。	△			0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合	仕様の対象としない	ベンダーによる提案事項	情報システムの開発用環境を設置しない	運用環境より機器構成を縮小した開発用環境を設置する	運用環境と同一の開発用環境を設置する				
C.4.2.1			試験用環境の設置有無	試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。	△		P52	2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [－] 開発用環境と試験用環境を併用する場合、または、情報システムの試験用環境を設置しない場合	仕様の対象としない	ベンダーによる提案事項	情報システムの試験用環境を設置しない	情報システムの開発用環境と併用する	専用の試験用環境を設置する				
C.5.9.1		サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○	○		3	四半期に1回	[－] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 障害発生時に実施される不定期の報告会は含まない。
C.5.9.2			報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○			1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○		P52	1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [－]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。
D.1.1.1	移行性	移行時期	システム移行期間	移行作業計画から本稼働までのシステム移行期間。	○			4	2年未満	年度を跨いで移行を進める必要がある。 [－] 期間短縮の場合 [+] さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	
D.1.1.3			並行稼働の有無	移行作業計画から本稼働までの並行稼働の有無。	○			1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [－] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。
E.3.1.2	セキュリティ	セキュリティ診断	Web診断実施の有無	Web診断とは、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。	○			1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [－] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	○	○	3	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [−] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	平常時、業務停止を伴う障害が発生した際には、	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	までのデータ復旧を目標とすること。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	○	○	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [−] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	平常時、業務停止を伴う障害が発生した際には、	6時間以内	でのシステム復旧を目標とすること。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	○	○	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [−] 影響を切り離せる機能がある場合	平常時、業務停止を伴う障害が発生した際には、	全システム機能の復旧	を実施すること。
A.1.4.1			システム再開目標（大規模災害時）	○	○	4	3日以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	大規模災害時、情報システムに甚大な被害が生じた場合、情報システムは、	3日以内に再開	することを目標とすること。
A.1.5.1			稼働率	○	○	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	年間のシステム稼働率は、	99.5%	を目標とすること。
A.2.1.1		耐障害性	冗長化※（サーバ機器）	△		2	すべてのサーバで冗長化※	すべてのサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムを構成する、サーバ機器については物理的に複数用意し、	すべてのサーバで冗長化※	をすること。
A.2.5.1			冗長化（ストレージ※機器）	△		2	すべての機器を冗長化※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	ネットワークを構成する伝送路（LANケーブル等）を物理的に複数用意し、	すべての機器を冗長化※	すること。
A.2.5.3			冗長化（ストレージ※のディスク）	△		1	RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	ハードディスクを物理的に複数台用意し、	RAID5※による冗長化※	をすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.3.1.1		災害対策	復旧方針	○		3	限定された構成をDRサイト※で構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	デスクアレイなどの外部記憶装置を物理的に複数台用意し、	限定された構成をDRサイト※で構築	すること。
A.3.2.1			保管場所分散度	○		2	1ヶ所 （遠隔地）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、	1ヶ所 （遠隔地）	とすること。
A.3.2.2			保管方法	○		2	DRサイト※へのリモートバックアップ※	遠隔地にリモートバックアップすることを推奨する。 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、	DRサイト※へのリモートバックアップ※	により、データ・プログラムを保管する場所を設置すること。
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	○		1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [−] 特定のユーザのみ使用することを合意できた場合	情報システムの利用者数は、	上限が決まっている	（●●●●人程度）。
B.1.1.2			同時アクセス数	○		1	同時アクセス※の上限が決まっている	情報システムに対してどのようなピークモデル※を想定しているか確認する。	情報システムの同時アクセス数は、	同時アクセス※の上限が決まっている	（●●●●人程度）。
B.1.1.3			データ量（項目・件数）	○		0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	情報システムは、	すべてのデータ量が明確である	（●●●●件程度）。
B.1.1.4			オンラインリクエスト件数※	○		0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	システムは、	処理ごとにリクエスト件数※が明確である	データ量の詳細は別添に記載のとおりとする。※データ量が明確である場合に記載
B.1.1.5			バッチ処理件数	○		0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	情報システムの業務処理件数は、	処理単位ごとに処理件数が決まっている	処理ごとのリクエスト件数の詳細は別添に記載のとおりとする。※リクエスト件数が明確である場合に記載
B.1.2.1			ユーザ数増大率	△		1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [−] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	情報システムのバッチ処理件数は、	1.2倍	の増大率に対応すること。
B.1.2.2			同時アクセス※数増大率	△		1	1.2倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [−] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加が相関関係でない場合 [+] 利用者の増加が見込まれる場合	情報システムは現状の同時アクセス数から、	1.2倍	の増大率に対応すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
B.1.2.3			データ量増大率	△		1	1.2倍	業務の手順によって情報システムで扱うデータ量がどの程度増加するかを確認する。 [-] データを蓄積しないゲートウェイシステムの場合 [+] 過去のデータを長期間保存する情報システムの場合	情報システムは現状のデータ量から、	1.2倍	の増大率に対応すること。
B.1.2.4			オンラインリクエスト件数※増大率	△		1	1.2倍	情報システムの制約となるリクエスト数※の見通しを確認する。	情報システムは現状のオンラインリクエスト件数から、	1.2倍	の増大率に対応すること。
B.1.2.5			バッチ処理件数増大率	△		1	1.2倍	情報システムの制約となる処理件数を確認する。	情報システムは現状のバッチ処理件数から、	1.2倍	の増大率に対応すること。
B.1.3.1			保管期間	△		3	5年	税制などの対応で保管期間が規定されているという想定。 [-] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	バックアップデータの保管期限は、	5年	とする。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	○	○	3	3秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	通常業務時のオンラインレスポンスタイムは、	3秒以内	を目標とすること。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※	○	○	2	5秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、	5秒以内	を目標とすること。
B.2.2.1			通常時バッチレスポンス※順守度合い	○	○	2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [-] 再実行をしない場合または代替手段がある場合	通常時のバッチレスポンスタイムは、	再実行の余裕が確保できる	ことを目標とする。
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い	○	○	2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時※のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時※に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [-] 再実行をしない場合または代替手段がある場合	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、	再実行の余裕が確保できる	ことを目標とする。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	○		1	定時内での利用（1日8時間程度利用）	主に、開庁時間内での利用を想定 [-] 不定期に利用するシステムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	情報システムの平日運用時間は、	定時内での利用（1日8時間程度利用）	を前提とすること。
C.1.1.2			運用時間（休日等）	○		0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	情報システムの休日運用時間は、	規定無し（原則利用しない）	を前提とすること。
C.1.2.2			外部データの利用可否	○		2	外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [-] 外部に同じデータを持つ情報システムが存在するため、本情報システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	データ復旧の際、	外部データは利用できない	とすること。
C.1.2.3			データ復旧の対応範囲	○		1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [-] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	データ復旧の対応範囲は、	障害発生時のデータ損失防止	とすること。
C.1.2.4			バックアップ自動化の範囲	-		2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [-] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	バックアップは、	1ステップのみ手動で行う（外部媒体交換のみ）	こと。
C.1.2.5			バックアップ取得間隔	○		4	日次で取得	全体バックアップは週次で取得する。しかし、RPO※要件である、1日前の状態に戻すためには、毎日差分バックアップ※を取得しなければならないことを想定。 [-] RPO※の要件が[-]される場合 [+] RPO※の要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	バックアップの取得間隔は、	日次で取得	すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.3.1			監視情報	○		3	エラー監視(トレース情報を含む)を行う	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムの監視については、	エラー監視(トレース情報を含む)を行う	こと。
C.2.3.5		保守運用	OS等パッチ※適用タイミング	○	○	4	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合(リスクの確認がとれている場合)。	OS等のパッチについては、	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	ことを目標とする。
C.3.3.1		障害時運用	対応可能時間	−		0	ベンダーの営業時間内(例:9時～17時)で対応を行う	[+]対応が必要な場合	システム異常検知時は、	ベンダーの営業時間内(例:9時～17時)で対応を行う	こと。
C.3.3.2			駆けつけ到着時間	−	○	4	保守員到着が異常検知から数時間内	[+]対応が必要な場合 [−]地理的条件・コスト等により、制限が有る場合。	システム異常時の駆けつけ到着時間は、	保守員到着が異常検知から数時間内	を目標とすること。
C.3.3.4			障害検知通知時間		○	0	障害を検知しない	本項目は、常駐保守または、サーバをデーターセンター※に設置した場合。 [+]対応が必要な場合		障害を検知しない	ため、利用者へ連絡は必要ない。
C.4.1.1		運用環境	開発用環境の設置有無	△		0	情報システムの開発用環境を設置しない	ベンダーの開発用環境(案件専用でない)による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合		情報システムの開発用環境を設置しない	こと。
C.4.2.1			試験用環境の設置有無	△		2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [−] 開発用環境と試験用環境を併用する場合、または、情報システムの試験用環境を設置しない場合	情報システムの試験用環境については、	専用の試験用環境を設置する	こと。
C.4.3.1			マニュアル準備レベル	○		2	情報システムの通常運用と保守運用のマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ※作業手順などを示した保守マニュアルも作成する。 [−] 保守作業はすべてベンダーに依頼するため、通常運用に必要なオペレーション※のみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	運用マニュアルについては、	情報システムの通常運用と保守運用のマニュアルを提供する	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.4.4.1		リモートオペレーション※	リモート監視※地点	－		1	庁内LANを介してリモート監視を行う	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [－] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	情報システムの監視形態は、	庁内LANを介してリモート監視を行う	こと。
C.4.4.3			リモート操作※時の接続方法	－		0	リモート操作※を行わない	仕様の対象としない	情報システムは、	リモート操作※を行わない	こと。
C.4.5.1		運用環境	外部システムとの接続有無	○		1	庁内の外部システムと接続する	庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [－] データのやり取りを行う多システムが存在しない場合 [+] 庁外のシステムに接続して、データのやり取りを行う場合	情報システムは、	庁内の外部システムと接続する	こと。
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	－		4	定額保守（オンサイト※）	オンサイト※の定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	ハードウェア保守については、	定額保守（オンサイト※）	とすること。
C.5.2.2			保守契約（ソフトウェア）の種類	○		2	アップデート※	ソフトウェアが法改正等によりバージョンアップ※した場合に、アップデートする権利を含めることを想定。 [－] アップデート※権を必要としない場合	情報システムのソフトウェア保守契約種類は、	アップデート※	をベンダーが実施すること。
C.5.3.1			ライフサイクル期間	△		1	5年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	情報システムのライフサイクル期間は、	5年	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.5.5.1			一次対応役割分担	－		2	すべてベンダーが実施	[−]ユーザにて一次切り分けが実施できるスキルが有る場合	一次対応については、	すべてベンダーが実施	とすること。
C.5.6.2			ベンダ側対応時間帯	－		1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [−]保守契約をしない場合	一次対応における対応時間は、	ベンダーの定時時間内（9～17時）	とすること。
C.5.9.1			定期報告会実施頻度	○	○	3	四半期に1回	[−] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	運用の定期報告は、	四半期に1回	程度実施すること。
C.5.9.2			報告内容のレベル	○		1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	保守の定期報告は、	障害報告のみ	実施すること。
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	○		1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [−]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	運用保守時の問い合わせ窓口については、	ベンダーの既設コールセンターを利用する	こと。
D.1.1.1	移行性	移行時期	システム移行期間	○		4	2年未満	年度を跨いで移行を進める必要がある。 [−] 期間短縮の場合 [+] さらに長期期間が必要な場合	既存システムから新システムへの移行期間は、	2年未満	とすること。
D.1.1.2			システム停止可能日時	○		4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [−] 停止を増やす場合	システム移行時のシステム停止可能日時は、	利用の少ない時間帯（夜間など）	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
D.1.1.3			並行稼働の有無	○		1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [−] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	システム移行時の並行稼働期間は、	有り	とすること。（●●ヶ月）
D.3.1.1		移行対象（機器）	設備・機器の移行内容	○		3	移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。 [−] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	現行システムで利用している、	移行対象設備・機器のシステム全部を入れ替える	こと。
D.4.1.1		移行対象（データ）	移行データ量	○		2	10TB未満	10TB（テラバイト）未満のデータを移行する必要がある。 [−] 1TB未満の場合 [+] 10TB以上の場合	現行システムから新システムへ	10TB未満	のデータを移行すること。
D.5.1.1		移行計画	移行のユーザ/ベンダ作業分担	○		1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	現行システムから新システムへのデータ移行作業は、	ユーザとベンダーと共同で実施	すること。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	○	○	1	有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	遵守すべき規程、ルール、法令、ガイドライン等は、	有り	とする。（●●●●）
E.2.1.1		セキュリティリスク分析	リスク分析範囲	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [−] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	システム開発実施において、セキュリティリスク分析を実施する範囲は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.3.1.2		セキュリティ診断	Web診断実施の有無	○		1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [−] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	情報システムのWeb診断は、	実施	すること。
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	○	○	2	定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	システム脆弱性等に対応するためのウィルス定義ファイルについては、	定義ファイルリリース時に実施	すること。
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	○		1	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	情報システムの認証方法は、	1回	とすること。
E.5.2.1			システム上の対策における操作制限度	○		1	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	情報システムへの操作制限は、	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	すること。
E.6.1.1		データの秘匿	伝送データの暗号化の有無	○		1	認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	伝送データについては、	認証情報のみ暗号化	すること。
E.6.1.2			蓄積データの暗号化の有無	○		1	認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	蓄積データについては、	認証情報のみ暗号化	すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.7.1.1		不正追跡・監視	ログ※の取得	○		1	必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	ログの取得については	必要なログを取得する	こと。
E.7.1.3			不正監視対象（装置）	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	不正監視対象は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	○		1	対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [-] Webアプリケーション※を用いない場合	セキュアコーディング、Webサーバの設定等は、	対策の強化	すること。
E.10.1.2			WAF※の導入の有無	○		0	無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	WAFの導入は、	無し	とすること。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	○		1	制約有り(重要な制約のみ適用)	庁内規約などが存在する場合を想定。 [-] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	システム構築時には、条例等の	制約有り(重要な制約のみ適用)	とすること。
F.1.2.1			運用時の制約条件	○		1	制約有り(重要な制約のみ適用)	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	システム運用時には、	制約有り(重要な制約のみ適用)	とすること。
F.2.2.1		システム特性	クライアント※数	△		1	上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合	情報システムで利用するクライアント数は、	上限が決まっている	こととする（●●●●人程度）。

Copyright © 2010-2014 IPA, LASDEC

活用シート【Ⅳ　全要求事項シート】

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
F.2.5.1			特定製品の採用有無	－		1	一部に特定製品の指定がある	構成する機器に関して固有の製品が指定された場合を想定。 [－] 特に指定がない場合	情報システムでは、	一部に特定製品の指定がある	こと。
F.3.1.1		適合規格	規格取得の有無(安全性)	－		1	規格取得の必要有り	機器の規格取得に関して指定があった場合を想定。 [－] 特に指定がない場合	情報システムはUL60950等の	規格取得の必要有り	とする。
F.3.2.1			規格取得の有無(有害物質)	△		1	RoHS指令※相当取得	RoHS指令※対応の装置が指定された場合を想定。 [－] 特に指定が無かった場合	情報システムでは、	RoHS指令※相当取得	すること。
F.5.1.1		環境マネージメント	グリーン購入法対応度	－		0	対処不要	団体の方針によるものと想定。 [+]団体の方針による。	情報システムのグリーン購入法については、	対処不要	とする。

Copyright © 2010-2014 IPA, LASDEC

非機能要求グレード活用シート
（地方公共団体版）

業務・情報システム分類グループ②

平成26年3月

財団法人　地方自治情報センター

[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及び財団法人地方自治情報センターが保有しています。

2. 本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものです。

3. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。詳細は、「利用ガイド」の「第3章　第8節 検討結果の情報システム調達仕様書への反映」をご参照ください。

4. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、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及び財団法人地方自治情報センターは、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又は財団法人地方自治情報センター又は第三者の著作権、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及び財団法人地方自治情報センターは、本資料のシステム開発への利用、開発された情報システムの使用、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、財団法人地方自治情報センターまでご連絡下さい。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○			2 外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [–] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				
C.2.3.5		保守運用	OS等パッチ※4適用タイミング	OS等パッチ※情報の展開とパッチ※適用のポリシー※に関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。	○	○	P29	4 緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [–]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチ※を適用しない	障害発生時にパッチ※適用を行う	定期保守時にパッチ※適用を行う	緊急性の高いパッチ※のみ即時に適用を行う	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチ※がリリースされるたびに適用を行う	【注意事項】 リリースされるパッチ※の種類（個別パッチ※／集合パッチ※）よって選択レベルが変わる場合がある。 セキュリティパッチ※については、セキュリティの項目でも検討すること（E.4.3.3）。
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	－		P30	1 庁内LANを介してリモート監視を行う	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [–] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。	－		P30	0 リモート操作※を行わない	ベンダーによるリモート操作はセキュリティの観点から実施を禁止していることを想定。 [+]サーバ等が複数拠点に分散する場合、または、設置場所がベンダーのサポート拠点から遠方にある場合	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				【注意事項】 リモート操作を実施できる範囲は、あらかじめ協議し決定しておく必要がある。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク など	○	○		1 有り	セキュリティポリシー等を順守する必要があることを想定。 [–] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り						【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、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。
E.2.1.1		セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクル※の確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [–] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	○	P30	2 定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [–]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。	○		P31	1 1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。
E.5.2.1			システム上の対策における操作制限度	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例）コマンド実行制,ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○			1 必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [–] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可					
E.6.1.1		データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。	○		P31	1 認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。
E.6.1.2			蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○		P32	1 認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化				【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.7.1.1		不正追跡・監視	ログ※の取得	不正を検知するために、監視のための記録（ログ※）を取得するかどうかの項目。 なお、どのようなログ※を取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログ※を取得する場合には、不正監視対象と併せて、取得したログ※のうち、確認する範囲を定める必要がある。	○			1 必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログ※は、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等
E.7.1.3			不正監視対象（装置）	サーバ、ストレージ※等への不正アクセス※等の監視のために、ログ※を取得する範囲を確認する。 不正行為を検知するために実施する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	Webアプリケーション※特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング※、Webサーバ※の設定等による対策の実施を検討する必要がある。	○		P32	1 対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [−] Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					【注意事項】 また、実施した結果の有効性を確認するための専門家のレビューやソースコード※診断、ツールによるチェック等についても検討する必要がある。 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。 Webシステムで考慮すべき項目。
E.10.1.2			WAF※の導入の有無	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。	○		P33	0 無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 Webシステムで考慮すべき項目。
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。	−		P33	1 規格取得の必要有り	機器の規格取得に関して指定があった場合を想定。 [−] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り					
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	△		P34	1 RoHS指令※相当取得	RoHS指令※対応の装置が指定された場合を想定。 [−] 特に指定が無かった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得					
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	−		P34	0 対処不要	団体の方針によるものと想定。 [+]団体の方針による。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　ー：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※4（業務停止時）	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情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	3	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [−] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P35	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [−] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P36	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [−] 影響を切り離せる機能がある場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）
A.1.4.1			システム再開目標（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	○	P37	2	一ヶ月以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1			稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	○	○	P38	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [−] 特定のユーザのみ使用することを合意できた場合	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				
B.1.1.2			同時アクセス数	同時アクセス※数とは、ある時点で情報システムにアクセス※しているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			1	同時アクセス※の上限が決まっている	情報システムに対してどのようなピークモデル※を想定しているか確認する。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセス※のみ	同時アクセス※の上限が決まっている	不特定多数のアクセス※有り				
B.1.1.3			データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○			0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ量が明確である	主要なデータ量のみが明確である					【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民基本台帳システムであれば住民データ・世帯データ・異動データ等がある。
B.1.1.4			オンラインリクエスト件数※	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数※が明確である	主な処理のリクエスト件数※のみが明確である					【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理などがある。
B.1.1.5			バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②			レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
B.1.2.1			ユーザ数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とユーザ数が最大になる時点のユーザ数の倍率。	△			1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [−] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.2			同時アクセス※数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点と同時アクセス数が最大になる時点の同時アクセス数の倍率。	△			1	1.2倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [−] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加が相関関係でない場合 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.3			データ量増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とデータ量が最大になる時点のデータ量の倍率。	△			1	1.2倍	業務の手順によって情報システムで扱うデータ量がどの程度増加するかを確認する。 [−] データを蓄積しないゲートウェイシステムの場合 [+] 過去のデータを長期間保存する情報システムの場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.4			オンラインリクエスト件数※増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とオンラインリクエスト件数が最大になる時点のオンラインリクエスト件の倍率。	△			1	1.2倍	情報システムの制約となるリクエスト数※の見通しを確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 オンラインリクエスト件数※は単位時間（1時間当たりの件数等）を明らかにして確認する。
B.1.2.5			バッチ処理件数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とバッチ処理件数が最大になる時点のバッチ処理件数の倍率。	△			1	1.2倍	情報システムの制約となる処理件数を確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 バッチ処理件数は単位時間（1日当たりの件数等）を明らかにして確認する。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	オンラインシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス※が必要かについて確認する。アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス※集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	○	P39	3	3秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [−] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※		○	○	P40	2	5秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [−] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.2.1			通常時バッチレスポンス※順守度合い	バッチシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム※）が必要かについて確認する。更に、アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時※・縮退運転※時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○	○		2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [−] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い		○	○		2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時※のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時※に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [−] 再実行をしない場合または代替手段がある場合	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	1 定時内での利用（1日8時間程度利用）	主に、開庁時間内での利用を想定 [–] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。
C.1.1.2			運用時間（休日等）	土日/祝祭日や年末年始に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	0 規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			
C.1.2.5			バックアップ取得間隔	バックアップ取得間隔	○		P41	4 日次で取得	全体バックアップは週次で取得する。しかし、RPO※要件である、1日前の状態に戻すためには、毎日差分バックアップ※を取得しなければならないことを想定。 [–] RPO※の要件が[–]される場合 [+] RPO※の要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	
C.3.3.1		障害時運用	対応可能時間	情報システムの異常検知時に保守員が作業対応を行う時間帯。	–			0 ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	ベンダーの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う				
C.3.3.2			駆けつけ到着時間	情報システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	–	○	P42	4 保守員到着が異常検知から数時間内	[+]対応が必要な場合 [–]地理的条件・コスト等により、制限が有る場合。	仕様の対象としない	ベンダーによる提案事項	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	
C.3.3.4			障害検知通知時間	障害の発生を検知した場合に、利用者（システム運用担当者）に通知するまでの時間。		○	P42	0 障害を検知しない	本項目は、常駐保守または、サーバをデーターセンター※に設置した場合。 [+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	障害を検知しない	24時間以内	8時間以内	3時間以内	1時間以内	30分以内	
C.4.3.1		運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○			2 情報システムの通常運用と保守運用のマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ※作業手順などを示した保守マニュアルも作成する。 [–] 保守作業はすべてベンダーに依頼するため、通常運用に必要なオペレーション※のみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ※収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。
C.4.5.1			外部システムとの接続有無	情報システムの運用に影響する外部システムとの接続の有無に関する項目。	○			1 庁内の外部システムと接続する	庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [–] データのやり取りを行う他システムが存在しない場合 [+] 庁外のシステムに接続して、データのやり取りを行う場合	仕様の対象としない	ベンダーによる提案事項	外部システムと接続しない	庁内の外部システムと接続する	庁外の外部システムと接続する				【注意事項】 接続する場合には、そのインターフェース※（接続ネットワーク・通信方式・データ形式等）について確認すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	保守が必要な対象ハードウェアに対する保守契約の種類。	－		P43	4 定額保守（オンサイト※）	オンサイト※の定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	随時保守（センドバック※）	定額保守（センドバック※）	随時保守（オンサイト※）	定額保守（オンサイト※）		
C.5.2.2			保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○			2 アップデート※	ソフトウェアが法改正等によりバージョンアップ※した場合に、アップデートする権利を含めることを想定。 [－] アップデート※権を必要としない場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート※				【注意事項】 アップデート権の範囲については、事前にベンダーと協議しておくこと。 ライフサイクル期間中に、OSやミドルウェアのバージョンアップが必要となる場合は、バージョンアップ後の情報システムの動作保障等についてあらかじめベンダーと協議しておくこと。 インターネットに公開する外部システムの場合は、最新ブラウザへの対応等についてもあらかじめベンダーと協議しておくこと。
C.5.3.1			ライフサイクル期間	運用保守の対応期間及び、実際に情報システムが稼動するライフサイクルの期間。ライフサイクルとは情報システムの利用期間(次回のシステム更改までの期間)のことを示している。	△		P44	1 5年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	仕様の対象としない	ベンダーによる提案事項	3年	5年	7年				【注意事項】 製品の保守可能期間よりも長い期間のライフサイクル※となる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。 【注意事項】 アプリケーションのパッケージソフトのライフサイクル※とは異なるので注意が必要。 通常のサポート期間は5年程度であり、それ以上の期間を求める場合には、コストの上昇を招くか、対応可能なベンダーが非常に限られるおそれがあるので注意が必要。 クラウド※の場合は、サービス提供可能期間として捉える。 【注意事項】 ライフサイクル期間中は、ソフトウェア・ハードウェアのサポート切れが発生しないようにする必要が有る。 クライアントPCとして、情報システム専用でない（例えば庁内LAN用に一括購入した）PCを使用する場合等は、更改時のOSバージョンアップ等についてあらかじめベンダーと協議しておくこと。
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダーの役割分担。	－			2 すべてベンダーが実施	[－]ユーザにて一次切り分けが実施できるスキルが有る場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザが実施	一部ユーザが実施	すべてベンダーが実施				
C.5.6.2			ベンダー側対応時間帯	一次対応のベンダーの対応時間。	－			1 ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [－]保守契約をしない場合	仕様の対象としない	ベンダーによる提案事項	対応無し	ベンダーの定時時間内（9～17時）	ユーザの指定する時間帯	24時間対応			
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	○			4 利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [－] 停止を増やす場合	仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。 レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○		P44	3 移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。 [－] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェア※を入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。	○		P45	2 10TB未満	10TB（テラバイト）未満のデータを移行する必要がある。 [－] 1TB未満の場合 [+] 10TB以上の場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上			
D.5.1.1		移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。	○			1 ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など	○			1 制約有り（重要な制約のみ適用）	庁内規約などが存在する場合を想定。 [−] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1			運用時の制約条件	運用時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク ・リモートからの運用の可否 など	○			1 制約有り（重要な制約のみ適用）	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				
F.2.2.1		システム特性	クライアント※数	情報システムで使用され、管理しなければいけないクライアント※（端末）の数。 専用端末、共用端末問わず、当該システムで使用するクライアント数を示す。	△			1 上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合	仕様の対象としない	ベンダーによる提案事項	特定クライアント※のみ	上限が決まっている	不特定多数のクライアント※が利用				
F.2.5.1		システム特性	特定製品の採用有無	ユーザの指定によるオープンソース※製品や第三者製品(独立系ソフトウェア会社/独立系ハードウェア会社)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。	―		P45	1 一部に特定製品の指定がある	構成する機器に関して固有の製品が指定された場合を想定。 [−] 特に指定がない場合	仕様の対象としない	ベンダーによる提案事項	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　ー：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
A.2.1.1	可用性	耐障害性	冗長化※4（サーバ機器）	サーバ機器を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	1 特定のサーバで冗長化※	特定のサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長※構成	特定のサーバで冗長化※	すべてのサーバで冗長化※				【レベル1】 特定のサーバで冗長化※とは、情報システムを構成するサーバの種別（DBサーバ※やAPサーバ※、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化※を指定する場合もある。
A.2.5.1			冗長化（ストレージ※機器）	ディスクアレイ※などの外部記憶装置を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	1 特定の機器のみ冗長化※	特定の機器のみ冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	特定の機器のみ冗長化※	すべての機器を冗長化※				【レベル1】 特定の機器のみとは、導入するストレージ※装置に格納するデータの重要度に応じて、耐障害性の要求が装置ごとに異なる場合を想定している。
A.2.5.3			冗長化（ストレージ※のディスク）	ハードディスクを物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P48	1 RAID5※による冗長化※	RAID5※による冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	RAID5※による冗長化※	RAID1※による冗長化※				【レベル2】 性能での要件からRAID0※との組み合わせを検討する。
A.3.1.1		災害対策	復旧方針	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための代替の機器として、どこに何が必要かを決める。	○		P48	2 同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイト※で構築	同一の構成をDRサイト※で構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化※の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。
A.3.2.1			保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管する。	○			2 1ヶ所（遠隔地）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（遠隔地）			【注意事項】 ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。
A.3.2.2			保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するための方法。	○		P49	0 媒体による保管	媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	媒体による保管	同一システム設置場所内の別ストレージ※へのバックアップ	DRサイト※へのリモートバックアップ※				
B.1.3.1	性能・拡張性	業務処理量	保管期間（データ）	情報システムが参照するデータのうち、OSやミドルウェア※のログ※などのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別ごとに定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	△			3 5年	税制などの対応で保管期間が規定されているという想定。 [−] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	仕様の対象としない	ベンダーによる提案事項	6ヶ月	1年	3年	5年	7年	10年以上有期	【レベル】 それぞれの情報システム（住民情報、税等）でデータの保管期間が異なる場合は、それぞれの対象データについて決めること。
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのような事象に対して対応する必要があるかを示す項目。	○		P50	1 障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	変更・削除したファイルの復旧				【注意事項】 職員の入力ミスを想定した変更・削除したファイルの復旧の場合、情報システムとしては正常に完了してしまった処理を元に戻さなければならないため、ファイルサーバ以外の情報システムでは実現できないと考えて良い。
C.1.2.4			バックアップ自動化の範囲	バックアップ自動化の範囲。 バックアップ運用には、 ・スケジュールに基づくジョブ起動※ ・バックアップ対象の選択 ・バックアップ先メディアの選択（外部媒体交換） ・ファイル転送 などといった作業ステップが存在する。別地保管を媒体搬送で行う場合の、外部媒体交換はここには含まない。	−		P50	2 1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	仕様の対象としない	ベンダーによる提案事項	全ステップを手動で行う	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンド※の入力）	1ステップのみ手動で行う（外部媒体交換のみ）	全ステップを自動で行う			

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ②		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.3.1			監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	○		P51	3	エラー監視（トレース情報を含む）を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [－] 障害時は管理者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] エラー情報だけでなく、リソース使用状況も監視して、障害発生を未然に防ぎたい場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータス※がオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報※を含む場合は、どのモジュール※でエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループット※について判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。
C.4.1.1		運用環境	開発用環境の設置有無	開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。 本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。	△			0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合	仕様の対象としない	ベンダーによる提案事項	情報システムの開発用環境を設置しない	運用環境より機器構成を縮小した開発用環境を設置する	運用環境と同一の開発用環境を設置する				
C.4.2.1			試験用環境の設置有無	試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。	△		P52	2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [－] 開発環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	仕様の対象としない	ベンダーによる提案事項	情報システムの試験用環境を設置しない	情報システムの開発用環境と併用する	専用の試験用環境を設置する				
C.5.9.1		サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○	○		3	四半期に1回	[－] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 障害発生時に実施される不定期の報告会は含まない。
C.5.9.2			報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○			1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○		P52	1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [－]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。
D.1.1.1	移行性	移行時期	システム移行期間	移行作業計画から本稼働までのシステム移行期間。	○			4	2年未満	年度を跨いで移行を進める必要がある。 [－] 期間短縮の場合 [+] さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	
D.1.1.3			並行稼働の有無	移行作業計画から本稼働までの並行稼働の有無。	○			1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [－] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。
E.3.1.2	セキュリティ	セキュリティ診断	Web診断実施の有無	Web診断とは、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。	○			1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [－] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	○	○	3	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	データの損失は許容できないため、障害発生時点までの復旧が原則。 [−] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定）	平常時、業務停止を伴う障害が発生した際には、	障害発生時点（日次バックアップ+アーカイブ※からの復旧）	までのデータ復旧を目標とすること。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	○	○	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [−] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	平常時、業務停止を伴う障害が発生した際には、	6時間以内	でのシステム復旧を目標とすること。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	○	○	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [−] 影響を切り離せる機能がある場合	平常時、業務停止を伴う障害が発生した際には、	全システム機能の復旧	を実施すること。
A.1.4.1			システム再開目標（大規模災害時）	○	○	2	一ヶ月以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	大規模災害時、情報システムに甚大な被害が生じた場合、情報システムは、	一ヶ月以内に再開	することを目標とすること。
A.1.5.1			稼働率	○	○	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	年間のシステム稼働率は、	99.5%	を目標とすること。
A.2.1.1		耐障害性	冗長化※（サーバ機器）	△		1	特定のサーバで冗長化※	特定のサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムを構成する、サーバ機器については物理的に複数用意し、	特定のサーバで冗長化※	をすること。
A.2.5.1			冗長化（ストレージ※機器）	△		1	特定の機器のみ冗長化※	特定の機器のみ冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	ネットワークを構成する伝送路（LANケーブル等）を物理的に複数用意し、	特定の機器のみ冗長化※	すること。
A.2.5.3			冗長化（ストレージ※のディスク）	△		1	RAID5※による冗長化※	RAID5※による冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	ハードディスクを物理的に複数台用意し、	RAID5※による冗長化※	をすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.3.1.1		災害対策	復旧方針	○		2	同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	デスクアレイなどの外部記憶装置を物理的に複数台用意し、	同一の構成で情報システムを再構築	すること。
A.3.2.1			保管場所分散度	○		2	1ヶ所 （遠隔地）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、	1ヶ所 （遠隔地）	とすること。
A.3.2.2			保管方法	○		0	媒体による保管	媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、	媒体による保管	により、データ・プログラムを保管する場所を設置すること。
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	○		1	上限が決まっている	あらかじめ一定の上限値を設定する場合を想定。 [−] 特定のユーザのみ使用することを合意できた場合	情報システムの利用者数は、	上限が決まっている	（●●●●人程度）。
B.1.1.2			同時アクセス数	○		1	同時アクセス※の上限が決まっている	情報システムに対してどのようなピークモデル※を想定しているか確認する。	情報システムの同時アクセス数は、	同時アクセス※の上限が決まっている	（●●●●人程度）。
B.1.1.3			データ量（項目・件数）	○		0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	情報システムは、	すべてのデータ量が明確である	（●●●●件程度）。
B.1.1.4			オンラインリクエスト件数※	○		0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	システムは、	処理ごとにリクエスト件数※が明確である	データ量の詳細は別添に記載のとおりとする。※データ量が明確である場合に記載
B.1.1.5			バッチ処理件数	○		0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	情報システムの業務処理件数は、	処理単位ごとに処理件数が決まっている	処理ごとのリクエスト件数の詳細は別添に記載のとおりとする。※リクエスト件数が明確である場合に記載
B.1.2.1			ユーザ数増大率	△		1	1.2倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [−] 利用者が固定されている場合 [+] 利用者の増加が見込まれる場合	情報システムのバッチ処理件数は、	1.2倍	の増大率に対応すること。
B.1.2.2			同時アクセス※数増大率	△		1	1.2倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [−] 利用者が固定されている場合やユーザの増加とアクセスユーザの増加が相関関係でない場合 [+] 利用者の増加が見込まれる場合	情報システムは現状の同時アクセス数から、	1.2倍	の増大率に対応すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
B.1.2.3			データ量増大率	△		1	1.2倍	業務の手順によって情報システムで扱うデータ量がどの程度増加するかを確認する。 [-] データを蓄積しないゲートウェイシステムの場合 [+] 過去のデータを長期間保存する情報システムの場合	情報システムは現状のデータ量から、	1.2倍	の増大率に対応すること。
B.1.2.4			オンラインリクエスト件数※増大率	△		1	1.2倍	情報システムの制約となるリクエスト数※の見通しを確認する。	情報システムは現状のオンラインリクエスト件数から、	1.2倍	の増大率に対応すること。
B.1.2.5			バッチ処理件数増大率	△		1	1.2倍	情報システムの制約となる処理件数を確認する。	情報システムは現状のバッチ処理件数から、	1.2倍	の増大率に対応すること。
B.1.3.1			保管期間	△		3	5年	税制などの対応で保管期間が規定されているという想定。 [-] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	バックアップデータの保管期限は、	5年	とする。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	○	○	3	3秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くても、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	通常業務時のオンラインレスポンスタイムは、	3秒以内	を目標とすること。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※	○	○	2	5秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良い場合。または代替手段がある場合 [+] 性能低下が、情報システムの評価低下につながる場合	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、	5秒以内	を目標とすること。
B.2.2.1			通常時バッチレスポンス※順守度合い	○	○	2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 [-] 再実行をしない場合または代替手段がある場合	通常時のバッチレスポンスタイムは、	再実行の余裕が確保できる	ことを目標とする。
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い	○	○	2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時※のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時※に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。 [-] 再実行をしない場合または代替手段がある場合	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、	再実行の余裕が確保できる	ことを目標とする。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	○		1	定時内での利用 （1日8時間程度利用）	主に、開庁時間内での利用を想定 [−] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	情報システムの平日運用時間は、	定時内での利用 （1日8時間程度利用）	を前提とすること。
C.1.1.2			運用時間（休日等）	○		0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	情報システムの休日運用時間は、	規定無し（原則利用しない）	を前提とすること。
C.1.2.2			外部データの利用可否	○		2	外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきて情報システムを復旧できるような場合	データ復旧の際、	外部データは利用できない	とすること。
C.1.2.3			データ復旧の対応範囲	○		1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	データ復旧の対応範囲は、	障害発生時のデータ損失防止	とすること。
C.1.2.4			バックアップ自動化の範囲	−		2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	バックアップは、	1ステップのみ手動で行う（外部媒体交換のみ）	こと。
C.1.2.5			バックアップ取得間隔	○		4	日次で取得	全体バックアップは週次で取得する。しかし、RPO※要件である、1日前の状態に戻すためには、毎日差分バックアップ※を取得しなければならないことを想定。 [−] RPO※の要件が[−]される場合 [+] RPO※の要件が[+]される場合や、複数世代を確保してバックアップの可用性を高めたい場合	バックアップの取得間隔は、	日次で取得	すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.3.1			監視情報	○		3	エラー監視(トレース情報を含む)を行う	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムの監視については、	エラー監視(トレース情報を含む)を行う	こと。
C.2.3.5		保守運用	OS等パッチ※適用タイミング	○	○	4	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合(リスクの確認がとれている場合)。	OS等のパッチについては、	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	ことを目標とする。
C.3.3.1		障害時運用	対応可能時間	−		0	ベンダーの営業時間内(例:9時～17時)で対応を行う	[+]対応が必要な場合	システム異常検知時は、	ベンダーの営業時間内(例:9時～17時)で対応を行う	こと。
C.3.3.2			駆けつけ到着時間	−	○	4	保守員到着が異常検知から数時間内	[+]対応が必要な場合 [−]地理的条件・コスト等により、制限が有る場合。	システム異常時の駆けつけ到着時間は、	保守員到着が異常検知から数時間内	を目標とすること。
C.3.3.4			障害検知通知時間		○	0	障害を検知しない	本項目は、常駐保守または、サーバをデーターセンター※に設置した場合。 [+]対応が必要な場合		障害を検知しない	ため、利用者へ連絡は必要ない。
C.4.1.1		運用環境	開発用環境の設置有無	△		0	情報システムの開発用環境を設置しない	ベンダーの開発用環境(案件専用でない)による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合		情報システムの開発用環境を設置しない	こと。
C.4.2.1			試験用環境の設置有無	△		2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [−] 開発環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	情報システムの試験用環境については、	専用の試験用環境を設置する	こと。
C.4.3.1			マニュアル準備レベル	○		2	情報システムの通常運用と保守運用のマニュアルを提供する	緊急時にはユーザ側にて保守対応を実施することも想定し、リカバリ※作業手順などを示した保守マニュアルも作成する。 [−] 保守作業はすべてベンダーに依頼するため、通常運用に必要なオペレーション※のみを説明した運用マニュアルのみ作成する場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	運用マニュアルについては、	情報システムの通常運用と保守運用のマニュアルを提供する	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.4.4.1		リモートオペレーション※	リモート監視※地点	－		1	庁内LANを介してリモート監視を行う	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [−] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	情報システムの監視形態は、	庁内LANを介してリモート監視を行う	こと。
C.4.4.3			リモート操作※時の接続方法	－		0	リモート操作※を行わない	仕様の対象としない	情報システムは、	リモート操作※を行わない	こと。
C.4.5.1		運用環境	外部システムとの接続有無	○		1	庁内の外部システムと接続する	庁内基幹系システムとして、住基と税などのように連携する庁内の他システムが存在することを想定。 [−] データのやり取りを行う他システムが存在しない場合 [+] 庁外のシステムに接続して、データのやり取りを行う場合	情報システムは、	庁内の外部システムと接続する	こと。
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	－		4	定額保守（オンサイト※）	オンサイト※の定額保守が地方公共団体の標準と想定。 [−] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	ハードウェア保守については、	定額保守（オンサイト※）	とすること。
C.5.2.2			保守契約（ソフトウェア）の種類	○		2	アップデート※	ソフトウェアが法改正等によりバージョンアップ※した場合に、アップデートする権利を含めることを想定。 [−] アップデート※権を必要としない場合	情報システムのソフトウェア保守契約種類は、	アップデート※	をベンダーが実施すること。
C.5.3.1			ライフサイクル期間	△		1	5年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [−] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	情報システムのライフサイクル期間は、	5年	とすること。
C.5.5.1			一次対応役割分担	－		2	すべてベンダーが実施	[−]ユーザにて一次切り分けが実施できるスキルが有る場合	一次対応については、	すべてベンダーが実施	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.5.6.2			ベンダ側対応時間帯	-		1	ベンダーの定時時間内（9～17時）	[+]運用時間帯に合わせて拡張する必要性がある場合 [-]保守契約をしない場合	一次対応における対応時間は、	ベンダーの定時時間内（9～17時）	とすること。
C.5.9.1			定期報告会実施頻度	○	○	3	四半期に1回	[-] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	運用の定期報告は、	四半期に1回	程度実施すること。
C.5.9.2			報告内容のレベル	○		1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	保守の定期報告は、	障害報告のみ	実施すること。
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	○		1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [-]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	運用保守時の問い合わせ窓口については、	ベンダーの既設コールセンターを利用する	こと。
D.1.1.1	移行性	移行時期	システム移行期間	○		4	2年未満	年度を跨いで移行を進める必要がある。 [-] 期間短縮の場合 [+] さらに長期期間が必要な場合	既存システムから新システムへの移行期間は、	2年未満	とすること。
D.1.1.2			システム停止可能日時	○		4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。 [-] 停止を増やす場合	システム移行時のシステム停止可能日時は、	利用の少ない時間帯（夜間など）	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
D.1.1.3			並行稼働の有無	○		1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [−] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	システム移行時の並行稼働期間は、	有り	とすること。（●●ヶ月）
D.3.1.1		移行対象（機器）	設備・機器の移行内容	○		3	移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。 [−] 業務アプリケーション更改が無い場合 [+] 業務アプリケーションの更改程度が大きい場合	現行システムで利用している、	移行対象設備・機器のシステム全部を入れ替える	こと。
D.4.1.1		移行対象（データ）	移行データ量	○		2	10TB未満	10TB（テラバイト）未満のデータを移行する必要がある。 [−] 1TB未満の場合 [+] 10TB以上の場合	現行システムから新システムへ	10TB未満	のデータを移行すること。
D.5.1.1		移行計画	移行のユーザ/ベンダ作業分担	○		1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	現行システムから新システムへのデータ移行作業は、	ユーザとベンダーと共同で実施	すること。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	○	○	1	有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	遵守すべき規程、ルール、法令、ガイドライン等は、	有り	とする。（●●●●）
E.2.1.1		セキュリティリスク分析	リスク分析範囲	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [−] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	システム開発実施において、セキュリティリスク分析を実施する範囲は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.3.1.2		セキュリティ診断	Web診断実施の有無	○		1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [–] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	情報システムのWeb診断は、	実施	すること。
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	○	○	2	定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [–]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	システム脆弱性等に対応するためのウィルス定義ファイルについては、	定義ファイルリリース時に実施	すること。
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	○		1	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	情報システムの認証方法は、	1回	とすること。
E.5.2.1			システム上の対策における操作制限度	○		1	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [–] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	情報システムへの操作制限は、	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	すること。
E.6.1.1		データの秘匿	伝送データの暗号化の有無	○		1	認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	伝送データについては、	認証情報のみ暗号化	すること。
E.6.1.2			蓄積データの暗号化の有無	○		1	認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	蓄積データについては、	認証情報のみ暗号化	すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.7.1.1		不正追跡・監視	ログ※の取得	○		1	必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	ログの取得については	必要なログを取得する	こと。
E.7.1.3			不正監視対象（装置）	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	不正監視対象は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	○		1	対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [−] Webアプリケーション※を用いない場合	セキュアコーディング、Webサーバの設定等は、	対策の強化	すること。
E.10.1.2			WAF※の導入の有無	○		0	無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	WAFの導入は、	無し	とすること。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	○		1	制約有り(重要な制約のみ適用)	庁内規約などが存在する場合を想定。 [−] 法や条例の制約を受けない場合、もしくは業界などの標準や取り決めなどがない場合	システム構築時には、条例等の	制約有り(重要な制約のみ適用)	とすること。
F.1.2.1			運用時の制約条件	○		1	制約有り(重要な制約のみ適用)	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	システム運用時には、	制約有り(重要な制約のみ適用)	とすること。

Copyright © 2010-2014 IPA, LASDEC

活用シート【Ⅳ　全要求事項シート】

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
F.2.2.1		システム特性	クライアント※数	△		1	上限が決まっている	あらかじめ一定の値を決めて合意することを想定。 [+] 上限台数を設定きない場合	情報システムで利用するクライアント数は、	上限が決まっている	こととする（●●●●人程度）。
F.2.5.1			特定製品の採用有無	－		1	一部に特定製品の指定がある	構成する機器に関して固有の製品が指定された場合を想定。 [－] 特に指定がない場合	情報システムでは、	一部に特定製品の指定がある	こと。
F.3.1.1		適合規格	規格取得の有無(安全性)	－		1	規格取得の必要有り	機器の規格取得に関して指定があった場合を想定。 [－] 特に指定がない場合	情報システムはUL60950等の	規格取得の必要有り	とする。
F.3.2.1			規格取得の有無（有害物質）	△		1	RoHS指令※相当取得	RoHS指令※対応の装置が指定された場合を想定。 [－] 特に指定が無かった場合	情報システムでは、	RoHS指令※相当取得	すること。
F.5.1.1		環境マネージメント	グリーン購入法対応度	－		0	対処不要	団体の方針によるものと想定。 [+]団体の方針による。	情報システムのグリーン購入法については、	対処不要	とする。

Copyright © 2010-2014 IPA, LASDEC

非機能要求グレード活用シート
（地方公共団体版）

業務・情報システム分類グループ③

2014年3月

財団法人　地方自治情報センター

[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及び財団法人地方自治情報センターが保有しています。

2. 本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものです。

3. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。詳細は、「利用ガイド」の「第3章　第8節 検討結果の情報システム調達仕様書への反映」をご参照ください。

4. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、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及び財団法人地方自治情報センターは、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又は財団法人地方自治情報センター又は第三者の著作権、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及び財団法人地方自治情報センターは、本資料のシステム開発への利用、開発された情報システムの使用、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、財団法人地方自治情報センターまでご連絡下さい。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○			1 一部のデータ復旧に利用できる	他システムから必要なデータを修復することができるため、バックアップによって情報システムの全データを復旧しなくてもよいことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、バックアップを取得しなくても本システムの全データを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				
C.2.3.5		保守運用	OS等パッチ※4適用タイミング	OS等パッチ※情報の展開とパッチ※適用のポリシー※に関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。	○	○	P29	4 緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチ※を適用しない	障害発生時にパッチ※適用を行う	定期保守時にパッチ※適用を行う	緊急性の高いパッチ※のみ即時に適用を行う	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチ※がリリースされるたびに適用を行う	【注意事項】 リリースされるパッチ※の種類（個別パッチ※／集合パッチ※）よって選択レベルが変わる場合がある。 セキュリティパッチ※については、セキュリティの項目でも検討すること（E.4.3.3）。
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	−		P30	0 リモート監視※を行わない	機器数が少ないため、リモートでの集中監視を行わない。 [+] 機器数が少なくとも、別途監視サーバを用意してリモート監視を行う場合	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。	−		P30	0 リモート操作※を行わない	ベンダーによるリモート操作はセキュリティの観点から実施を禁止していることを想定。 [+]サーバ等が複数拠点に分散する場合、または、設置場所がベンダーのサポート拠点から遠方にある場合	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				【注意事項】 リモート操作を実施できる範囲は、あらかじめ協議し決定しておく必要がある。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク など	○	○		1 有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り						【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、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。
E.2.1.1		セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクル※の確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○			0 分析なし	詳細なリスク分析は実施しないが、基本的な対策は実施する。	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	○	P30	2 定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。	○		P31	1 1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。
E.5.2.1			システム上の対策における操作制限度	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例）コマンド実行制,ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○			1 必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可					
E.6.1.1		データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。	○		P31	1 認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [−] 認証情報をネットワークを経由して送信しない場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。
E.6.1.2			蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○		P32	1 認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [−] 認証を実施しない場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化				【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.7.1.1		不正追跡・監視	ログ※の取得	不正を検知するために、監視のための記録（ログ※）を取得するかどうかの項目。 なお、どのようなログ※を取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログ※を取得する場合には、不正監視対象と併せて、取得したログ※のうち、確認する範囲を定める必要がある。	○			1 必要なログを取得する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある）	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログ※は、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等
E.7.1.3			不正監視対象（装置）	サーバ、ストレージ※等への不正アクセス※等の監視のために、ログ※を取得する範囲を確認する。 不正行為を検知するために実施する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	Webアプリケーション※特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング※、Webサーバ※の設定等による対策の実施を検討する必要がある。	○		P32	1 対策の強化	外部システムについては必須。 内部システムについても、今後対策を実施した製品の増加が想定される。 [−] 内部システム向けのパッケージに、対策を実施している製品が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					【注意事項】 また、実施した結果の有効性を確認するための専門家のレビューやソースコード※診断、ツールによるチェック等についても検討する必要がある。 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。 Webシステムで考慮すべき項目。
E.10.1.2			WAF※の導入の有無	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。	○		P33	0 無し	内部ネットワークのみ接続するシステムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 Webシステムで考慮すべき項目。
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。	−		P33	0 規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り					
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	△		P34	0 規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得					
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	−		P34	0 対処不要	団体の方針によるものと想定。 [+]団体の方針による。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	-	*	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※[4]（業務停止時）	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情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	1	5営業日前の時点（週次バックアップからの復旧）	データの損失はある程度許容でき、週次のバックアップからの復旧とする。 [−] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P35	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [−] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P36	1	一部システム機能の復旧	一部機能のみを対象とすることができる場合を想定。 [+] 機能毎に影響を切り離せない場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）
A.1.4.1			システム再開目標（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	○	P37	4	3日以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1			稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	○	○	P38	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			0	特定ユーザのみ	部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				
B.1.1.2			同時アクセス数	同時アクセス※数とは、ある時点で情報システムにアクセス※しているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			0	特定利用者の限られたアクセス※のみ	登録ユーザから想定する。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセス※のみ	同時アクセス※の上限が決まっている	不特定多数のアクセス※有り				
B.1.1.3			データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○			0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ量が明確である	主要なデータ量のみが明確である					【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民基本台帳システムであれば住民データ・世帯データ・異動データ等がある。
B.1.1.4			オンラインリクエスト件数※	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数※が明確である	主な処理のリクエスト件数※のみが明確である					【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理などがある。
B.1.1.5			バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	-	*	0	1	2	3	4	5	
B.1.2.1			ユーザ数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とユーザ数が最大になる時点のユーザ数の倍率。	△			0	1倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.2			同時アクセス※数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点と同時アクセス数が最大になる時点の同時アクセス数の倍率。	△			0	1倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.3			データ量増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とデータ量が最大になる時点のデータ量の倍率。	△			0	1倍	業務のトレンドによって情報システムで扱うデータ量がどの程度増加するかを確認する。 [+] 段階的稼働や、マスター蓄積システムの場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.4			オンラインリクエスト件数※増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とオンラインリクエスト件数が最大になる時点のオンラインリクエスト件の倍率。	△			0	1倍	情報システムの制約となるリクエスト数※の見通しを確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 オンラインリクエスト件数※は単位時間（1時間当たりの件数等）を明らかにして確認する。
B.1.2.5			バッチ処理件数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とバッチ処理件数が最大になる時点のバッチ処理件数の倍率。	△			0	1倍	情報システムの制約となる処理件数を確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 バッチ処理件数は単位時間（1日当たりの件数等）を明らかにして確認する。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	オンラインシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス※が必要かについて確認する。アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス※集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	○	P39	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※		○	○	P40	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.2.1			通常時バッチレスポンス※順守度合い	バッチシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム※）が必要かについて確認する。更に、アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時※・縮退運転※時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○	○		0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い		○	○		0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス※順守度に関しては特に規定しないと想定。	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	1 定時内での利用（1日8時間程度利用）	主に、開庁時間内での利用を想定 [−] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。
C.1.1.2			運用時間（休日等）	土日/祝祭日や年末年始に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	0 規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			
C.1.2.5			バックアップ取得間隔	バックアップ取得間隔	○		P41	1 システム構成の変更時など、任意のタイミング	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	
C.3.3.1		障害時運用	対応可能時間	情報システムの異常検知時に保守員が作業対応を行う時間帯。	−			0 ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	ベンダーの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う				
C.3.3.2			駆けつけ到着時間	情報システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	−	○	P42	3 保守員到着が異常検知からユーザの翌営業開始時まで	[+]対応が必要な場合 [−]地理的条件・コスト等により、制限が有る場合。	仕様の対象としない	ベンダーによる提案事項	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	
C.3.3.4			障害検知通知時間	障害の発生を検知した場合に、利用者（システム運用担当者）に通知するまでの時間。		○	P42	0 障害を検知しない	常駐保守または、サーバをデータセンター※に設置した場合には必要となる。 [+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	障害を検知しない	24時間以内	8時間以内	3時間以内	1時間以内	30分以内	
C.4.3.1		運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○			0 各製品標準のマニュアルを利用する	情報システムの操作方法について、管理者が製品マニュアルを参照して習得することを想定。必要に応じて、ユーザが運用マニュアルを作成する。 [+] ベンダーよりマニュアルの提供を受ける必要がある場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。障害発生時の一次対応に関する記述（系切り替え作業やログ※収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。
C.4.5.1			外部システムとの接続有無	情報システムの運用に影響する外部システムとの接続の有無に関する項目。	○			0 外部システムと接続しない	部門内システムであり、連携する他システムが存在しない。 [+] 連携する他システムが存在する場合	仕様の対象としない	ベンダーによる提案事項	外部システムと接続しない	庁内の外部システムと接続する	庁外の外部システムと接続する				【注意事項】 接続する場合には、そのインターフェース※（接続ネットワーク・通信方式・データ形式等）について確認すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	保守が必要な対象ハードウェアに対する保守契約の種類。	－		P43	4	定額保守（オンサイト※）	オンサイトの定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	随時保守（センドバック※）	定額保守（センドバック※）	随時保守（オンサイト※）	定額保守（オンサイト※）		
C.5.2.2			保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○			1	問い合わせ対応	法改正対応等によるバージョンアップが少ないため、問い合わせ対応のみを想定。 [－] アップデート権を必要とする場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート※				【注意事項】 アップデート権の範囲については、事前にベンダーと協議しておくこと。 ライフサイクル期間中に、OSやミドルウェアのバージョンアップが必要となる場合は、バージョンアップ後の情報システムの動作保障等についてあらかじめベンダーと協議しておくこと。 インターネットに公開する外部システムの場合は、最新ブラウザへの対応等についてもあらかじめベンダーと協議しておくこと。
C.5.3.1			ライフサイクル期間	運用保守の対応期間及び、実際に情報システムが稼動するライフサイクルの期間。ライフサイクルとは情報システムの利用期間（次回のシステム更改までの期間）のことを示している。	△		P44	1	5年	導入するハードウェア・ソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	仕様の対象としない	ベンダーによる提案事項	3年	5年	7年				【注意事項】 製品の保守可能期間よりも長い期間のライフサイクル※となる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。 【注意事項】 アプリケーションのパッケージソフトのライフサイクル※とは異なるので注意が必要。 通常のサポート期間は5年程度であり、それ以上の期間を求める場合には、コストの上昇を招くか、対応可能なベンダーが非常に限られるおそれがあるので注意が必要。 クラウド※の場合は、サービス提供可能期間として捉える。 【注意事項】 ライフサイクル期間中は、ソフトウェア・ハードウェアのサポート切れが発生しないようにする必要が有る。 クライアントPCとして、情報システム専用でない（例えば庁内LAN用に一括購入した）PCを使用する場合等は、更改時のOSバージョンアップ等についてあらかじめベンダーと協議しておくこと。
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダーの役割分担。	－			2	すべてベンダーが実施	[－]ユーザにて一次切り分けが実施できるスキルが有る場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザが実施	一部ユーザが実施	すべてベンダーが実施				
C.5.6.2			ベンダー側対応時間帯	一次対応のベンダーの対応時間。	－			1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [－]保守契約をしない場合	仕様の対象としない	ベンダーによる提案事項	対応無し	ベンダーの定時時間内（9～17時）	ユーザの指定する時間帯	24時間対応			
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	○			1	5日以上	業務への影響が少なく数日以上はシステム停止可能。 [－] さらに停止を多くする場合 [+] 停止を少なくする場合	仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。 レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○		P44	0	移行対象無し	設備機器を新設する必要がある。 [+] 既存設備機器が存在する場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェア※を入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。	○		P45	1	1TB未満	1TB（テラバイト）未満のデータ（マスター等）を移行する必要がある。 [+] 1TB以上の場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上			
D.5.1.1		移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。	○			1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など	○			0	制約無し	特に制限などを受けない場合を想定。 [+] 法や条例の制約を受ける場合、もしくは業界などの標準や取り決めなどがある場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1			運用時の制約条件	運用時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク ・リモートからの運用の可否 など	○			0	制約無し	特に制限などを受けない場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				
F.2.2.1		システム特性	クライアント※数	情報システムで使用され、管理しなければいけないクライアント※（端末）の数。 専用端末、共用端末問わず、当該システムで使用するクライアント数を示す。	△			0	特定クライアント※のみ	特定のクライアントのみが使用することを想定。 [+] 将来的にクライアント数の増加が予想され、上限値で合意が必要な場合	仕様の対象としない	ベンダーによる提案事項	特定クライアント※のみ	上限が決まっている	不特定多数のクライアント※が利用				
F.2.5.1		システム特性	特定製品の採用有無	ユーザの指定によるオープンソース※製品や第三者製品(独立系ソフトウェア会社/独立系ハードウェア会社)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。	―		P45	0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　ー：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
A.2.1.1	可用性	耐障害性	冗長化※4（サーバ機器）	サーバ機器を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	1 特定のサーバで冗長化※	特定のサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長※構成	特定のサーバで冗長化※	すべてのサーバで冗長化※				【レベル1】 特定のサーバで冗長化※とは、情報システムを構成するサーバの種別（DBサーバ※やAPサーバ※、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化※を指定する場合もある。
A.2.5.1			冗長化（ストレージ※機器）	ディスクアレイ※などの外部記憶装置を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	1 特定の機器のみ冗長化※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	特定の機器のみ冗長化※	すべての機器を冗長化※				【レベル1】 特定の機器のみとは、導入するストレージ※装置に格納するデータの重要度に応じて、耐障害性の要求が装置ごとに異なる場合を想定している。
A.2.5.3			冗長化（ストレージ※のディスク）	ハードディスクを物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P48	1 RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	RAID5※による冗長化※	RAID1※による冗長化※				【レベル2】 性能での要件からRAID0※との組み合わせを検討する。
A.3.1.1		災害対策	復旧方針	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための代替の機器として、どこに何が必要かを決める。	○		P48	3 限定された構成をDRサイト※で構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイト※で構築	同一の構成をDRサイト※で構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化※の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。
A.3.2.1			保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管する。	○			1 1ヶ所（近隣の別な建物）	同一敷地内の別な建物等への保管を想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（遠隔地）			【注意事項】 ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。
A.3.2.2			保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するための方法。	○		P49	0 媒体による保管	媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	媒体による保管	同一システム設置場所内の別ストレージ※へのバックアップ	DRサイト※へのリモートバックアップ※				
B.1.3.1	性能・拡張性	業務処理量	保管期間（データ）	情報システムが参照するデータのうち、OSやミドルウェア※のログ※などのシステム基盤が利用するデータに対する保管が必要な期間。 必要に応じて、データの種別ごとに定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	△			1 1年	毎年データを更新していく想定。 [−] 保管データがほとんど無い場合 [+] ディスク容量に余裕がある場合	仕様の対象としない	ベンダーによる提案事項	6ヶ月	1年	3年	5年	7年	10年以上有期	【レベル】 それぞれの情報システム（住民情報、税等）でデータの保管期間が異なる場合は、それぞれの対象データについて決めること。
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのような事象に対して対応する必要があるかを示す項目。	○		P50	1 障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	変更・削除したファイルの復旧				【注意事項】 職員の入力ミスを想定した変更・削除したファイルの復旧の場合、情報システムとしては正常に完了してしまった処理を元に戻さなければならないため、ファイルサーバ以外の情報システムでは実現できないと考えて良い。
C.1.2.4			バックアップ自動化の範囲	バックアップ自動化の範囲。 バックアップ運用には、 ・スケジュールに基づくジョブ起動※ ・バックアップ対象の選択 ・バックアップ先メディアの選択（外部媒体交換） ・ファイル転送 などといった作業ステップが存在する。別地保管を媒体搬送で行う場合の、外部媒体交換はここには含まない。	−		P50	2 1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	仕様の対象としない	ベンダーによる提案事項	全ステップを手動で行う	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンド※の入力）	1ステップのみ手動で行う（外部媒体交換のみ）	全ステップを自動で行う			

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ③		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.3.1			監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	○		P51	2	エラー監視を行う	管理者がすぐに情報システムにアクセスして障害状況を調査することができるため、エラーが発生したことのみを通知できればよい。 [−] ハードウェアやプロセスの死活状態のみが判断できれば良いような場合 [+] 障害対応時間の短縮のため、管理者が情報システムにアクセスしなくても、ある程度障害箇所が判断できるようにする必要がある場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータス※がオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報※を含む場合は、どのモジュール※でエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループット※について判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。
C.4.1.1		運用環境	開発用環境の設置有無	開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。 本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。	△			0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合	仕様の対象としない	ベンダーによる提案事項	情報システムの開発用環境を設置しない	運用環境より機器構成を縮小した開発用環境を設置する	運用環境と同一の開発用環境を設置する				
C.4.2.1			試験用環境の設置有無	試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。	△		P52	2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [−] 開発用環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	仕様の対象としない	ベンダーによる提案事項	情報システムの試験用環境を設置しない	情報システムの開発用環境と併用する	専用の試験用環境を設置する				
C.5.9.1		サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○	○		3	四半期に1回	[−] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 障害発生時に実施される不定期の報告会は含まない。
C.5.9.2			報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○			1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○		P52	1	ベンダーの既設コールセンターを利用する	ユーザ/ベンダー間のやり取りに関してサービスデスク機能を設けず、個別対応にすることを想定 [+] サービスデスクを設置する場合	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。
D.1.1.1	移行性	移行時期	システム移行期間	移行作業計画から本稼働までのシステム移行期間。	○			1	3ヶ月未満	情報システムを短期間で構築する必要がある。 [+] 中長期間で進める場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	
D.1.1.3			並行稼働の有無	移行作業計画から本稼働までの並行稼働の有無。	○			0	無し	移行のためのシステム停止期間も十分確保できるため並行稼働の必要性は低い。 [+] 移行のためのシステム停止期間が確保できず、並行稼働する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。
E.3.1.2	セキュリティ	セキュリティ診断	Web診断実施の有無	Web診断とは、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。	○			1	実施	ネットワークを通じた不特定多数の攻撃者からの脅威にさらされる。そのため、Webアプリケーション※に関する脆弱性を分析する必要がある。 [−] Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	○	○	1	5営業日前の時点（週次バックアップからの復旧）	データの損失はある程度許容でき、週次のバックアップからの復旧とする。 [−] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	平常時、業務停止を伴う障害が発生した際には、	5営業日前の時点（週次バックアップからの復旧）	までのデータ復旧を目標とすること。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	○	○	3	6時間以内	なるべく早く復旧する。故障時すみやかに利用可能な予備機を使用した復旧を想定。 [−] 業務停止の影響が小さい場合 [+] コストと地理的条件等の実現性を確認した上で、復旧時間を短縮したい場合	平常時、業務停止を伴う障害が発生した際には、	6時間以内	でのシステム復旧を目標とすること。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	○	○	1	一部システム機能の復旧	一部機能のみを対象とすることができる場合を想定。 [+] 機能毎に影響を切り離せない場合	平常時、業務停止を伴う障害が発生した際には、	一部システム機能の復旧	を実施すること。
A.1.4.1			システム再開目標（大規模災害時）	○	○	4	3日以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	大規模災害時、情報システムに甚大な被害が生じた場合、情報システムは、	3日以内に再開	することを目標とすること。
A.1.5.1			稼働率	○	○	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	年間のシステム稼働率は、	99.5%	を目標とすること。
A.2.1.1		耐障害性	冗長化※（サーバ機器）	△		1	特定のサーバで冗長化※	特定のサーバで冗長化※ [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムを構成する、サーバ機器については物理的に複数用意し、	特定のサーバで冗長化※	をすること。
A.2.5.1			冗長化（ストレージ※機器）	△		1	特定の機器のみ冗長化※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	ネットワークを構成する伝送路（LANケーブル等）を物理的に複数用意し、	特定の機器のみ冗長化※	すること。
A.2.5.3			冗長化（ストレージ※のディスク）	△		1	RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	ハードディスクを物理的に複数台用意し、	RAID5※による冗長化※	をすること。

Copyright © 2010-2014 IPA, LASDEC

活用シート【Ⅳ　全要求事項シート】

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.3.1.1		災害対策	復旧方針	○		3	限定された構成をDRサイト※で構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	デスクアレイなどの外部記憶装置を物理的に複数台用意し、	限定された構成をDRサイト※で構築	すること。
A.3.2.1			保管場所分散度	○		1	1ヶ所 （近隣の別な建物）	同一敷地内の別な建物等への保管を想定 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、	1ヶ所 （近隣の別な建物）	とすること。
A.3.2.2			保管方法	○		0	媒体による保管	媒体による保管を想定。 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、	媒体による保管	により、データ・プログラムを保管する場所を設置すること。
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	○		0	特定ユーザのみ	部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	情報システムの利用者数は、	特定ユーザのみ	とする。（●●●●人程度）。
B.1.1.2			同時アクセス数	○		0	特定利用者の限られたアクセス※のみ	登録ユーザから想定する。	情報システムの同時アクセス数は、	特定利用者の限られたアクセス※のみ	とする。（●●●●人程度）。
B.1.1.3			データ量（項目・件数）	○		0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	情報システムは、	すべてのデータ量が明確である	（●●●●件程度）。
B.1.1.4			オンラインリクエスト件数※	○		0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	システムは、	処理ごとにリクエスト件数※が明確である	データ量の詳細は別添に記載のとおりとする。※データ量が明確である場合に記載
B.1.1.5			バッチ処理件数	○		0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	情報システムの業務処理件数は、	処理単位ごとに処理件数が決まっている	処理ごとのリクエスト件数の詳細は別添に記載のとおりとする。※リクエスト件数が明確である場合に記載
B.1.2.1			ユーザ数増大率	△		0	1倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [+] 利用者の増加が見込まれる場合	情報システムのバッチ処理件数は、	1倍	とすること。
B.1.2.2			同時アクセス※数増大率	△		0	1倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [+] 利用者の増加が見込まれる場合	情報システムは現状の同時アクセス数から、	1倍	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
B.1.2.3			データ量増大率	△		0	1倍	業務のトレンドによって情報システムで扱うデータ量がどの程度増加するかを確認する。 [+] 段階的稼働や、マスター蓄積システムの場合	情報システムは現状のデータ量から、	1倍	とすること。
B.1.2.4			オンラインリクエスト件数※増大率	△		0	1倍	情報システムの制約となるリクエスト数※の見通しを確認する。	情報システムは現状のオンラインリクエスト件数から、	1倍	とすること。
B.1.2.5			バッチ処理件数増大率	△		0	1倍	情報システムの制約となる処理件数を確認する。	情報システムは現状のバッチ処理件数から、	1倍	とすること。
B.1.3.1			保管期間	△		1	1年	毎年データを更新していく想定。 [-] 保管データがほとんど無い場合 [+] ディスク容量に余裕がある場合	バックアップデータの保管期限は、	1年	とする。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	○	○	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	通常業務時のオンラインレスポンスタイムは、	規定しない	。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※	○	○	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、	規定しない	。
B.2.2.1			通常時バッチレスポンス※順守度合い	○	○	0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	通常時のバッチレスポンスタイムは、	順守度合いを定めない	こと。
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い	○	○	0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス※順守度に関しては特に規定しないと想定。	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、	順守度合いを定めない	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	○		1	定時内での利用 （1日8時間程度利用）	主に、開庁時間内での利用を想定 [−] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	情報システムの平日運用時間は、	定時内での利用 （1日8時間程度利用）	を前提とすること。
C.1.1.2			運用時間（休日等）	○		0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	情報システムの休日運用時間は、	規定無し（原則利用しない）	を前提とすること。
C.1.2.2			外部データの利用可否	○		1	一部のデータ復旧に利用できる	他システムから必要なデータを修復することができるため、バックアップによって情報システムの全データを復旧しなくてもよいことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、バックアップを取得しなくても本システムの全データを復旧できるような場合	データ復旧の際、外部データの利用は、	一部のデータ復旧に利用できる	こと。
C.1.2.3			データ復旧の対応範囲	○		1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	データ復旧の対応範囲は、	障害発生時のデータ損失防止	とすること。
C.1.2.4			バックアップ自動化の範囲	−		2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	バックアップは、	1ステップのみ手動で行う（外部媒体交換のみ）	こと。
C.1.2.5			バックアップ取得間隔	○		1	システム構成の変更時など、任意のタイミング	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	バックアップの取得間隔は、	システム構成の変更時など、任意のタイミング	とすること。

Copyright © 2010−2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.3.1			監視情報	○		2	エラー監視を行う	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムの監視については、	エラー監視を行う	こと。
C.2.3.5		保守運用	OS等パッチ※適用タイミング	○	○	4	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	OS等のパッチについては、	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	ことを目標とする。
C.3.3.1		障害時運用	対応可能時間	−		0	ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	システム異常検知時は、	ベンダーの営業時間内（例：9時～17時）で対応を行う	こと。
C.3.3.2			駆けつけ到着時間	−	○	3	保守員到着が異常検知からユーザの翌営業開始時まで	[+]対応が必要な場合 [−]地理的条件・コスト等により、制限が有る場合。	システム異常時の駆けつけ到着時間は、	保守員到着が異常検知からユーザの翌営業開始時まで	を目標とすること。
C.3.3.4			障害検知通知時間		○	0	障害を検知しない	常駐保守または、サーバをデータセンター※に設置した場合には必要となる。 [+]対応が必要な場合		障害を検知しない	ため、利用者へ連絡は必要ない。
C.4.1.1		運用環境	開発用環境の設置有無	△		0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合		情報システムの開発用環境を設置しない	こと。
C.4.2.1			試験用環境の設置有無	△		2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [−] 開発用環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	情報システムの試験用環境については、	専用の試験用環境を設置する	こと。
C.4.3.1			マニュアル準備レベル	○		0	各製品標準のマニュアルを利用する	情報システムの操作方法について、管理者が製品マニュアルを参照して習得することを想定。必要に応じて、ユーザが運用マニュアルを作成する。 [+] ベンダーよりマニュアルの提供を受ける必要がある場合	運用マニュアルについては、	各製品標準のマニュアルを利用する	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.4.4.1		リモートオペレーション※	リモート監視※地点	－		0	リモート監視※を行わない	機器数が少ないため、リモートでの集中監視を行わない。 [+] 機器数が少なくとも、別途監視サーバを用意してリモート監視を行う場合	情報システムの監視形態は、	リモート監視※を行わない	こと。
C.4.4.3			リモート操作※時の接続方法	－		0	リモート操作※を行わない	仕様の対象としない	情報システムは、	リモート操作※を行わない	こと。
C.4.5.1		運用環境	外部システムとの接続有無	○		0	外部システムと接続しない	部門内システムであり、連携する他システムが存在しない。 [+] 連携する他システムが存在する場合		外部システムと接続しない	こと。
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	－		4	定額保守（オンサイト※）	オンサイトの定額保守が地方公共団体の標準と想定。 [−] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	ハードウェア保守については、	定額保守（オンサイト※）	とすること。
C.5.2.2			保守契約（ソフトウェア）の種類	○		1	問い合わせ対応	法改正対応等によるバージョンアップが少ないため、問い合わせ対応のみを想定。 [−] アップデート権を必要とする場合	情報システムのソフトウェア保守契約種類は、	問い合わせ対応	をベンダーが実施すること。
C.5.3.1			ライフサイクル期間	△		1	5年	導入するハードウェア・ソフトウェアのサポート期間に合わせて情報システムのライフサイクル※を5年と決定したと想定。 [−] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	情報システムのライフサイクル期間は、	5年	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.5.5.1			一次対応役割分担	－		2	すべてベンダーが実施	[−]ユーザにて一次切り分けが実施できるスキルが有る場合	一次対応については、	すべてベンダーが実施	とすること。
C.5.6.2			ベンダ側対応時間帯	－		1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [−]保守契約をしない場合	一次対応における対応時間は、	ベンダーの定時時間内（9～17時）	とすること。
C.5.9.1			定期報告会実施頻度	○	○	3	四半期に1回	[−] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	運用の定期報告は、	四半期に1回	程度実施すること。
C.5.9.2			報告内容のレベル	○		1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	保守の定期報告は、	障害報告のみ	実施すること。
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	○		1	ベンダーの既設コールセンターを利用する	ユーザ/ベンダー間のやり取りに関してサービスデスク機能を設けず、個別対応にすることを想定 [+] サービスデスクを設置する場合	運用保守時の問い合わせ窓口については、	ベンダーの既設コールセンターを利用する	こと。
D.1.1.1	移行性	移行時期	システム移行期間	○		1	3ヶ月未満	情報システムを短期間で構築する必要がある。 [+] 中長期間で進める場合	既存システムから新システムへの移行期間は、	3ヶ月未満	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
D.1.1.2			システム停止可能日時	○		1	5日以上	業務への影響が少なく数日以上はシステム停止可能。 [-] さらに停止を多くする場合 [+] 停止を少なくする場合	システム移行時のシステム停止可能日時は、	5日以上	とすること。
D.1.1.3			並行稼働の有無	○		0	無し	移行のためのシステム停止期間も十分確保できるため並行稼働の必要性は低い。 [+] 移行のためのシステム停止期間が確保できず、並行稼働する場合	システム移行時の並行稼働期間は、	無し	とすること。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	○		0	移行対象無し	設備機器を新設する必要がある。 [+] 既存設備機器が存在する場合	現行システムで利用している設備・機器は、	移行対象無し	とする。
D.4.1.1		移行対象（データ）	移行データ量	○		1	1TB未満	1TB（テラバイト）未満のデータ（マスター等）を移行する必要がある。 [+] 1TB以上の場合	現行システムから新システムへ	1TB未満	のデータを移行すること。
D.5.1.1		移行計画	移行のユーザ/ベンダ作業分担	○		1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	現行システムから新システムへのデータ移行作業は、	ユーザとベンダーと共同で実施	すること。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき社内規程、ルール、法令、ガイドライン等の有無	○	○	1	有り	セキュリティポリシー等を順守する必要があることを想定。 [-] 順守すべき規程やルール、法令、ガイドライン等が無い場合	遵守すべき規程、ルール、法令、ガイドライン等は、	有り	とする。（●●●●）

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.2.1.1		セキュリティリスク分析	リスク分析範囲	○		0	分析なし	詳細なリスク分析は実施しないが、基本的な対策は実施する。	システム開発実施において、セキュリティリスクの	分析なし	とすること。
E.3.1.2		セキュリティ診断	Web診断実施の有無	○		1	実施	ネットワークを通じた不特定多数の攻撃者からの脅威にさらされる。そのため、Webアプリケーション※に関する脆弱性を分析する必要がある。 [−] Webアプリケーション※を用いない場合	情報システムのWeb診断は、	実施	すること。
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	○	○	2	定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	システム脆弱性等に対応するためのウィルス定義ファイルについては、	定義ファイルリリース時に実施	すること。
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	○		1	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	情報システムの認証方法は、	1回	とすること。
E.5.2.1			システム上の対策における操作制限度	○		1	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	情報システムへの操作制限は、	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	すること。
E.6.1.1		データの秘匿	伝送データの暗号化の有無	○		1	認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [−] 認証情報をネットワークを経由して送信しない場合	伝送データについては、	認証情報のみ暗号化	すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.6.1.2			蓄積データの暗号化の有無	○		1	認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [-] 認証を実施しない場合	蓄積データについては、	認証情報のみ暗号化	すること。
E.7.1.1		不正追跡・監視	ログ※の取得	○		1	必要なログを取得する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。 （ログ取得の処理を実行することにより、性能に影響する可能性がある）	ログの取得については	必要なログを取得する	こと。
E.7.1.3			不正監視対象（装置）	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。	不正監視対象は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	○		1	対策の強化	外部システムについては必須。 内部システムについても、今後対策を実施した製品の増加が想定される。 [-] 内部システム向けのパッケージに、対策を実施している製品が無い場合	セキュアコーディング、Webサーバの設定等は、	対策の強化	すること。
E.10.1.2			WAF※の導入の有無	○		0	無し	内部ネットワークのみ接続するシステムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	WAFの導入は、	無し	とすること。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	○		0	制約無し	特に制限などを受けない場合を想定。 [+] 法や条例の制約を受ける場合、もしくは業界などの標準や取り決めなどがある場合	システム構築時には、条例等の	制約無し	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
F.1.2.1			運用時の制約条件	○		0	制約無し	特に制限などを受けない場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	システム運用時には、	制約無し	とすること。
F.2.2.1		システム特性	クライアント※数	△		0	特定クライアント※のみ	特定のクライアントのみが使用することを想定。 [+] 将来的にクライアント数の増加が予想され、上限値で合意が必要な場合	情報システムで利用するクライアント数は、	特定クライアント※のみ	とすること。（●●●●人程度）。
F.2.5.1			特定製品の採用有無	－		0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合	情報システムでは、	特定製品の指定がない	。
F.3.1.1		適合規格	規格取得の有無(安全性)	－		0	規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合	情報システムはUL60950等の	規格取得の必要無し	とする。
F.3.2.1			規格取得の有無（有害物質）	△		0	規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合	情報システムでは、	規格取得の必要無し	とする。
F.5.1.1		環境マネージメント	グリーン購入法対応度	－		0	対処不要	団体の方針によるものと想定。 [+]団体の方針による。	情報システムのグリーン購入法については、	対処不要	とする。

Copyright © 2010-2014 IPA, LASDEC

非機能要求グレード活用シート
（地方公共団体版）

業務・情報システム分類グループ④

平成26年3月

財団法人　地方自治情報センター

[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及び財団法人地方自治情報センターが保有しています。

2. 本資料は、独立行政法人情報処理推進機構が作成した「非機能要求グレード」を財団法人地方自治情報センターが地方公共団体向けに一部変更したものです。

3. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、「本資料の全部又は一部を複製、改変、公衆送信、又は翻訳/翻案し、第三者に有償又は無償で再配布すること」を許諾します。なお、複製し再配布する場合は本使用条件を添付し、本使用条件に記載されている条件を配布先に遵守させて下さい。改変又は翻訳/翻案し再配布する場合は、新しく使用条件を設定することが可能ですが、本使用条件を必ず含めて下さい。詳細は、「利用ガイド」の「第3章　第8節 検討結果の情報システム調達仕様書への反映」をご参照ください。

4. 独立行政法人情報処理推進機構及び財団法人地方自治情報センターは、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及び財団法人地方自治情報センターは、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又は財団法人地方自治情報センター又は第三者の著作権、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及び財団法人地方自治情報センターは、本資料のシステム開発への利用、開発された情報システムの使用、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、財団法人地方自治情報センターまでご連絡下さい。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○			1	一部のデータ復旧に利用できる	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきてシステムを復旧できるような場合	仕様の対象としない	ベンダーによる提案事項	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				
C.2.3.5		保守運用	OS等パッチ※4適用タイミング	OS等パッチ※情報の展開とパッチ※適用のポリシー※に関する項目。 OS等は、OS、ミドルウェア、その他のソフトウェアを指す。	○	○	P29	4	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	仕様の対象としない	ベンダーによる提案事項	パッチ※を適用しない	障害発生時にパッチ※適用を行う	定期保守時にパッチ※適用を行う	緊急性の高いパッチ※のみ即時に適用を行う	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチ※がリリースされるたびに適用を行う	【注意事項】 リリースされるパッチ※の種類（個別パッチ※／集合パッチ※）よって選択レベルが変わる場合がある。 セキュリティパッチ※については、セキュリティの項目でも検討すること（E.4.3.3）。
C.4.4.1		リモートオペレーション※	リモート監視※地点	情報システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。	−		P30	0	リモート監視※を行わない	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [−] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	仕様の対象としない	ベンダーによる提案事項	リモート監視※を行わない	庁内LANを介してリモート監視を行う	ベンダー拠点等外部からリモート監視を行う				【レベル】 監視の内容については、通常運用の運用監視の項目にて確認する必要がある。
C.4.4.3			リモート操作※時の接続方法	ベンダーがリモート監視※地点からリモート操作を実施する場合の回線接続方法。	−		P30	0	リモート操作※を行わない	ベンダーによるリモート操作はセキュリティの観点から実施を禁止していることを想定。 [+]サーバ等が複数拠点に分散する場合、または、設置場所がベンダーのサポート拠点から遠方にある場合	仕様の対象としない	ベンダーによる提案事項	リモート操作※を行わない	リモート操作※の必要時のみ接続する	常時接続環境にてリモート操作※を行う				【注意事項】 リモート操作を実施できる範囲は、あらかじめ協議し決定しておく必要がある。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが順守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク など	○	○		1	有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、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。
E.2.1.1		セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクル※の確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○			0	分析なし	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [−] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				【レベル1】 外接部分とは、インターネットへの接続部分や、外部へ情報を持ち出す際に用いる媒体等を接続する部分、また、外部システムとデータのやりとりを行う部分等を意味する。 なお、以降のレベルにおいても同様の意味で用いている。 重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	○	P30	2 定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回の認証を実施することにより、抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生態認証等がある。	○		P31	1 1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。
E.5.2.1			システム上の対策における操作制限度	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例）コマンド実行制,ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○			1 必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可					
E.6.1.1		データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。	○		P31	1 認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。
E.6.1.2			蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○		P32	1 認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化				【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
E.7.1.1		不正追跡・監視	ログ※の取得	不正を検知するために、監視のための記録（ログ※）を取得するかどうかの項目。 なお、どのようなログ※を取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログ※を取得する場合には、不正監視対象と併せて、取得したログ※のうち、確認する範囲を定める必要がある。	○			1 必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログ※は、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等
E.7.1.3			不正監視対象（装置）	サーバ、ストレージ※等への不正アクセス※等の監視のために、ログ※を取得する範囲を確認する。 不正行為を検知するために実施する。	○			1 重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	Webアプリケーション※特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング※、Webサーバ※の設定等による対策の実施を検討する必要がある。	○		P32	1 対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [−] Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					【注意事項】 また、実施した結果の有効性を確認するための専門家のレビューやソースコード※診断、ツールによるチェック等についても検討する必要がある。 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。 Webシステムで考慮すべき項目。
E.10.1.2			WAF※の導入の有無	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。	○		P33	0 無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 Webシステムで考慮すべき項目。
F.3.1.1	システム環境・エコロジー	適合規格	規格取得の有無(安全性)	提供する情報システムに使用する製品について、UL60950※などの製品安全規格を取得していることを要求されているかを確認する項目。	−		P33	0 規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	規格取得の必要有り					
F.3.2.1			規格取得の有無（有害物質）	提供する情報システムに使用する製品について、RoHS指令※などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。	△		P34	0 規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	規格取得の必要無し	RoHS指令※相当取得					
F.5.1.1		環境マネージメント	グリーン購入法対応度	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材・消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。	−		P34	0 対処不要	団体の方針によるものと想定。 [+]団体の方針による。	仕様の対象としない	ベンダーによる提案事項	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　ー：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※4（業務停止時）	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情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	○	P35	1	5営業日前の時点（週次バックアップからの復旧）	データの損失はある程度許容でき、週次のバックアップからの復旧とする。 [−] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブ※からの復旧）			【注意事項】 RLO※で業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P35	1	1営業日以内	故障したハードウェアを交換し、バックアップ媒体により環境やデータを復旧することを想定。 [−] 業務停止の影響が小さい場合 [+] 業務停止の影響が大きい場合	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	○	P36	1	一部システム機能の復旧	一部機能のみを対象とすることができる場合を想定。 [+] 機能ごとに影響を切り離せない場合	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合等。）
A.1.4.1			システム再開目標（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	○	P37	1	数ヶ月以内に再開	災害発生後、あらかじめ準備した代替え機やクラウドサービス等を利用し、新たにシステム環境を構築することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1			稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。	○	○	P38	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			0	特定ユーザのみ	部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				
B.1.1.2			同時アクセス数	同時アクセス※数とは、ある時点で情報システムにアクセス※しているユーザ数のことである。パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○			0	特定利用者の限られたアクセス※のみ	登録ユーザから想定する。	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセス※のみ	同時アクセス※の上限が決まっている	不特定多数のアクセス※有り				
B.1.1.3			データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○			0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	すべてのデータ量が明確である	主要なデータ量のみが明確である				【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民基本台帳システムであれば住民データ・世帯データ・異動データ等がある。
B.1.1.4			オンラインリクエスト件数※	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数※が明確である	主な処理のリクエスト件数※のみが明確である				【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民情報システムの転入・転出処理などがある。
B.1.1.5			バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○			0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている				【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第４章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
B.1.2.1			ユーザ数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とユーザ数が最大になる時点のユーザ数の倍率。	△			0	1倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.2			同時アクセス※数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点と同時アクセス数が最大になる時点の同時アクセス数の倍率。	△			0	1倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [+] 利用者の増加が見込まれる場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.3			データ量増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とデータ量が最大になる時点のデータ量の倍率。	△			0	1倍	業務のトレンドによって情報システムで扱うデータ量がどの程度増加するかを確認する。 [+] 段階的稼働や、マスター蓄積システムの場合	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 減少が予測される場合は、レベル0（1倍）を選択する。
B.1.2.4			オンラインリクエスト件数※増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とオンラインリクエスト件数が最大になる時点のオンラインリクエスト件の倍率。	△			0	1倍	情報システムの制約となるリクエスト数※の見通しを確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 オンラインリクエスト件数※は単位時間（1時間当たりの件数等）を明らかにして確認する。
B.1.2.5			バッチ処理件数増大率	システム稼動開始からライフサイクル※終了までの間で、開始時点とバッチ処理件数が最大になる時点のバッチ処理件数の倍率。	△			0	1倍	情報システムの制約となる処理件数を確認する。	仕様の対象としない	ベンダーによる提案事項	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	【注意事項】 バッチ処理件数は単位時間（1日当たりの件数等）を明らかにして確認する。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	オンラインシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス※が必要かについて確認する。アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス※集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	○	P39	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※		○	○	P40	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.2.1			通常時バッチレスポンス※順守度合い	バッチシステム利用時に要求されるレスポンス※。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム※）が必要かについて確認する。更に、アクセス※が集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時※・縮退運転※時ごとに順守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○	○		0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い		○	○		0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	仕様の対象としない	ベンダーによる提案事項	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	-	*	0	1	2	3	4	5	
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	1	定時内での利用（1日8時間程度利用）	主に、開庁時間内での利用を想定 [-] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。
C.1.1.2			運用時間（休日等）	土日/祝祭日や年末年始に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○		P40	0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			
C.1.2.5			バックアップ取得間隔	バックアップ取得間隔	○		P41	1	システム構成の変更時など、任意のタイミング	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	
C.3.3.1		障害時運用	対応可能時間	情報システムの異常検知時に保守員が作業対応を行う時間帯。	－			0	ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	ベンダーの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24時間対応を行う				
C.3.3.2			駆けつけ到着時間	情報システムの異常を検出してから、指定された連絡先への通知、保守員が障害連絡を受けて現地へ到着するまでの時間。	－	○	P42	3	保守員到着が異常検知からユーザの翌営業開始時まで	[+]対応が必要な場合 [-]地理的条件・コスト等により、制限が有る場合。	仕様の対象としない	ベンダーによる提案事項	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐	
C.3.3.4			障害検知通知時間	障害の発生を検知した場合に、利用者（システム運用担当者）に通知するまでの時間。		○	P42	0	障害を検知しない	常駐保守または、サーバをデータセンター※に設置した場合には必要となる。 [+]対応が必要な場合	仕様の対象としない	ベンダーによる提案事項	障害を検知しない	24時間以内	8時間以内	3時間以内	1時間以内	30分以内	
C.4.3.1		運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○			0	各製品標準のマニュアルを利用する	情報システムの操作方法について、管理者が製品マニュアルを参照して習得することを想定。必要に応じて、ユーザが運用マニュアルを作成する。 [+] ベンダーよりマニュアルの提供を受ける必要がある場合	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ※収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。
C.4.5.1			外部システムとの接続有無	情報システムの運用に影響する外部システムとの接続の有無に関する項目。	○			0	外部システムと接続しない	部門内システムであり、連携する他システムが存在しない。 [+]連携する他システムが存在する場合	仕様の対象としない	ベンダーによる提案事項	外部システムと接続しない	庁内の外部システムと接続する	庁外の外部システムと接続する				【注意事項】 接続する場合には、そのインターフェース※（接続ネットワーク・通信方式・データ形式等）について確認すること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	保守が必要な対象ハードウェアに対する保守契約の種類。	－		P43	4	定額保守（オンサイト※）	オンサイトの定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	随時保守（センドバック※）	定額保守（センドバック※）	随時保守（オンサイト※）	定額保守（オンサイト※）		
C.5.2.2			保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○			1	問い合わせ対応	情報システムを構成する個々のソフトウェア製品を調達し、SIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート※				【注意事項】 アップデート権の範囲については、事前にベンダーと協議しておくこと。 ライフサイクル期間中に、OSやミドルウェアのバージョンアップが必要となる場合は、バージョンアップ後の情報システムの動作保障等についてあらかじめベンダーと協議しておくこと。 インターネットに公開する外部システムの場合は、最新ブラウザへの対応等についてもあらかじめベンダーと協議しておくこと。
C.5.3.1			ライフサイクル期間	運用保守の対応期間及び、実際に情報システムが稼動するライフサイクルの期間。ライフサイクルとは情報システムの利用期間(次回の情報システム更改までの期間)のことを示している。	△		P44	1	5年	導入するハードウェア・ソフトウェアのサポート期間に合わせて情報システムのライフサイクルを5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	仕様の対象としない	ベンダーによる提案事項	3年	5年	7年				【注意事項】 製品の保守可能期間よりも長い期間のライフサイクル※となる場合は、保守延長や保守可能バージョンへのアップ等の対応が必要となる。 【注意事項】 アプリケーションのパッケージソフトのライフサイクル※とは異なるので注意が必要。 通常のサポート期間は5年程度であり、それ以上の期間を求める場合には、コストの上昇を招くか、対応可能なベンダーが非常に限られるおそれがあるので注意が必要。 クラウド※の場合は、サービス提供可能期間として捉える。 【注意事項】 ライフサイクル期間中は、ソフトウェア・ハードウェアのサポート切れが発生しないようにする必要が有る。 クライアントPCとして、情報システム専用でない（例えば庁内LAN用に一括購入した）PCを使用する場合等は、更改時のOSバージョンアップ等についてあらかじめベンダーと協議しておくこと。
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダーの役割分担。	－			2	すべてベンダーが実施	[－]ユーザにて一次切り分けが実施できるスキルが有る場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザが実施	一部ユーザが実施	すべてベンダーが実施				
C.5.6.2			ベンダー側対応時間帯	一次対応のベンダーの対応時間。	－			1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [－] 保守契約をしない場合	仕様の対象としない	ベンダーによる提案事項	対応無し	ベンダーの定時時間内（9～17時）	ユーザの指定する時間帯	24時間対応			
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	○			1	5日以上	業務への影響が少なく数日以上はシステム停止可能。 [－] さらに停止を多くする場合 [+] 停止を少なくする場合	仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 情報システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。（例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。） その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。 レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○		P44	0	移行対象無し	設備機器を新設する必要がある。 [+] 既存設備機器が存在する場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェア※を入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。	○		P45	1	1TB未満	1TB（テラバイト）未満のデータ（マスター等）を移行する必要がある。 [+] 1TB以上の場合	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上			
D.5.1.1		移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。	○			1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。 【注意事項】 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限 など	○			0	制約無し	特に制限などを受けない場合を想定。 [+] 法や条例の制約を受ける場合、もしくは業界などの標準や取り決めなどがある場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1			運用時の制約条件	運用時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準 ・プライバシーマーク ・リモートからの運用の可否 など	○			0	制約無し	特に制限などを受けない場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）				
F.2.2.1		システム特性	クライアント※数	情報システムで使用され、管理しなければいけないクライアント※（端末）の数。 専用端末、共用端末問わず、当該システムで使用するクライアント数を示す。	△			0	特定クライアント※のみ	特定のクライアントのみが使用することを想定。 [+] 将来的にクライアント数の増加が予想され、上限値で合意が必要な場合	仕様の対象としない	ベンダーによる提案事項	特定クライアント※のみ	上限が決まっている	不特定多数のクライアント※が利用				
F.2.5.1		システム特性	特定製品の採用有無	ユーザの指定によるオープンソース※製品や第三者製品(独立系ソフトウェア会社/独立系ハードウェア会社)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。	―		P45	0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合	仕様の対象としない	ベンダーによる提案事項	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④			レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル		選択時の条件	－	＊	0	1	2	3	4	5	
A.2.1.1	可用性	耐障害性	冗長化※4（サーバ機器）	サーバ機器を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	0	非冗長※構成	冗長化※しない [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長※構成	特定のサーバで冗長化※	すべてのサーバで冗長化※				【レベル1】 特定のサーバで冗長化※とは、情報システムを構成するサーバの種別（DBサーバ※やAPサーバ※、監視サーバなど）で冗長化の対応を分けることを意味する。 また要求としてサーバの単位ではなく、業務や機能の単位で冗長化※を指定する場合もある。
A.2.5.1			冗長化（ストレージ※機器）	ディスクアレイ※などの外部記憶装置を物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P47	0	非冗長構成※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	特定の機器のみ冗長化※	すべての機器を冗長化※				【レベル1】 特定の機器のみとは、導入するストレージ※装置に格納するデータの重要度に応じて、耐障害性の要求が装置ごとに異なる場合を想定している。
A.2.5.3			冗長化（ストレージ※のディスク）	ハードディスクを物理的に複数用意し、1台が故障しても他方で稼働が可能な状態にすること。 ハードウェア構成を決定するために必要。	△		P48	1	RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	非冗長構成※	RAID5※による冗長化※	RAID1※による冗長化※				【レベル2】 性能での要件からRAID0※との組み合わせを検討する。
A.3.1.1		災害対策	復旧方針	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための代替の機器として、どこに何が必要かを決める。	○		P48	2	同一の構成で情報システムを再構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイト※で構築	同一の構成をDRサイト※で構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化※の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。
A.3.2.1			保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管する。	○			1	1ヶ所（近隣の別な建物）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（遠隔地）			【注意事項】 ここで遠隔地とは、サーバ等の設置場所から見ての遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。
A.3.2.2			保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するための方法。	○		P49	0	媒体による保管	遠隔地にリモートバックアップすることを推奨する。 [+] コストと実現性を確認した上で、可用性を高めたい場合	仕様の対象としない	ベンダーによる提案事項	媒体による保管	同一システム設置場所内の別ストレージ※へのバックアップ	DRサイト※へのリモートバックアップ※				
B.1.3.1	性能・拡張性	業務処理量	保管期間（データ）	情報システムが参照するデータのうち、OSやミドルウェア※のログ※などのシステム基盤が利用するデータに対する保管が必要な期間。必要に応じて、データの種別ごとに定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。	△			1	1年	税制などの対応で保管期間が規定されているという想定。 [−] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	仕様の対象としない	ベンダーによる提案事項	6ヶ月	1年	3年	5年	7年	10年以上有期	【レベル】 それぞれの情報システム（住民情報、税等）でデータの保管期間が異なる場合は、それぞれの対象データについて決めること。
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのような事象に対して対応する必要があるかを示す項目。	○		P50	1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	変更・削除したファイルの復旧				【注意事項】 職員の入力ミスを想定した変更・削除したファイルの復旧の場合、情報システムとしては正常に完了してしまった処理を元に戻さなければならないため、ファイルサーバ以外の情報システムでは実現できないと考えて良い。
C.1.2.4			バックアップ自動化の範囲	バックアップ自動化の範囲。 バックアップ運用には、 ・スケジュールに基づくジョブ起動※ ・バックアップ対象の選択 ・バックアップ先メディアの選択（外部媒体交換） ・ファイル転送 などといった作業ステップが存在する。別地保管を媒体搬送で行う場合の、外部媒体交換はここには含まない。	−		P50	2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	仕様の対象としない	ベンダーによる提案事項	全ステップを手動で行う	数ステップを手動で行う（外部媒体交換とバックアップ開始コマンド※の入力）	1ステップのみ手動で行う（外部媒体交換のみ）	全ステップを自動で行う			

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	検収時の扱い[2]	利用ガイドの解説[3]	グループ④		レベル								備考 ［利用ガイド］第4章も参照のこと
								選択レベル	選択時の条件	－	＊	0	1	2	3	4	5	
C.1.3.1			監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	○		P51	2	エラー監視を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [－] 障害時は管理者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] エラー情報だけでなく、リソース使用状況も監視して、障害発生を未然に防ぎたい場合	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視（トレース情報を含む）を行う	リソース監視を行う	パフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータス※がオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報※を含む場合は、どのモジュール※でエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループット※について判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。
C.4.1.1		運用環境	開発用環境の設置有無	開発用環境とは、本番環境とは別に開発専用に使用することのできる機材一式のことを指す。 本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。	△			0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合	仕様の対象としない	ベンダーによる提案事項	情報システムの開発用環境を設置しない	運用環境より機器構成を縮小した開発用環境を設置する	運用環境と同一の開発用環境を設置する				
C.4.2.1			試験用環境の設置有無	試験用環境とは、本番環境とは別に試験専用に使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。	△		P52	2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [－] 開発環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	仕様の対象としない	ベンダーによる提案事項	情報システムの試験用環境を設置しない	情報システムの開発用環境と併用する	専用の試験用環境を設置する				
C.5.9.1		サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○	○		3	四半期に1回	[－] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 障害発生時に実施される不定期の報告会は含まない。
C.5.9.2			報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○			1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○		P52	1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [－]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。
D.1.1.1	移行性	移行時期	システム移行期間	移行作業計画から本稼働までのシステム移行期間。	○			1	3ヶ月未満	年度を跨いで移行を進める必要がある。 [－] 期間短縮の場合 [+] さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	
D.1.1.3			並行稼働の有無	移行作業計画から本稼働までの並行稼働の有無。	○			0	無し	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [－] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、場所等を規定すること。
E.3.1.2	セキュリティ	セキュリティ診断	Web診断実施の有無	Web診断とは、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。	○			1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [－] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 詳細は、当センターの「地方公共団体における情報システムセキュリティ要求仕様モデルプラン」を参照の上、対策を検討すること。

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目　なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 検収時の扱い　○：目標（値）として扱い、長期的に測定・評価を行うべき項目

3 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

4 「※」が付記された用語　利用ガイド及び調査報告書の用語集にて解説のあるIT専門用語

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.1.3.1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	○	○	1	5営業日前の時点（週次バックアップからの復旧）	データの損失はある程度許容でき、週次のバックアップからの復旧とする。 [−] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	平常時、業務停止を伴う障害が発生した際には、	5営業日前の時点（週次バックアップからの復旧）	までのデータ復旧を目標とすること。
A.1.3.2			RTO（目標復旧時間）※（業務停止時）	○	○	1	1営業日以内	故障したハードウェアを交換し、バックアップ媒体により環境やデータを復旧することを想定。 [−] 業務停止の影響が小さい場合 [+] 業務停止の影響が大きい場合	平常時、業務停止を伴う障害が発生した際には、	1営業日以内	でのシステム復旧を目標とすること。
A.1.3.3			RLO（目標復旧レベル）※（業務停止時）	○	○	1	一部システム機能の復旧	一部機能のみを対象とすることができる場合を想定。 [+] 機能ごとに影響を切り離せない場合	平常時、業務停止を伴う障害が発生した際には、	一部システム機能の復旧	を実施すること。
A.1.4.1			システム再開目標（大規模災害時）	○	○	1	数ヶ月以内に再開	災害発生後、あらかじめ準備した代替え機やクラウドサービス等を利用し、新たにシステム環境を構築することを想定。機能は、業務が再開できる最低限の機能に限定する。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	大規模災害時、情報システムに甚大な被害が生じた場合、情報システムは、	数ヶ月以内に再開	することを目標とすること。
A.1.5.1			稼働率	○	○	3	99.5%	ベンダーのサポート拠点から、車で2時間程度の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [+] コストと地理的条件等の実現性を確認した上で、可用性を高めたい場合 [−]地理的条件から実現困難な場合。業務停止が許容できる場合。	年間のシステム稼働率は、	99.5%	を目標とすること。
A.2.1.1		耐障害性	冗長化※（サーバ機器）	△		0	非冗長※構成	冗長化※しない [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムを構成する、サーバ機器については物理的に複数用意し、	非冗長※構成	とすること。
A.2.5.1			冗長化（ストレージ※機器）	△		0	非冗長構成※	すべての機器を冗長化※ [+] コストと実現性を確認した上で、可用性※を高めたい場合	ネットワークを構成する伝送路（LANケーブル等）を物理的に複数用意し、	非冗長構成※	とすること。
A.2.5.3			冗長化（ストレージ※のディスク）	△		1	RAID5※による冗長化※	RAID5※による冗長化 [+] コストと実現性を確認した上で、可用性を高めたい場合	ハードディスクを物理的に複数台用意し、	RAID5※による冗長化※	をすること。

Copyright © 2010-2014 IPA, LASDEC

活用シート【Ⅳ　全要求事項シート】

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
A.3.1.1		災害対策	復旧方針	○		2	同一の構成で情報システムを再構築	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	デスクアレイなどの外部記憶装置を物理的に複数台用意し、	同一の構成で情報システムを再構築	すること。
A.3.2.1			保管場所分散度	○		1	1ヶ所 （近隣の別な建物）	遠隔地1ヵ所 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、	1ヶ所 （近隣の別な建物）	とすること。
A.3.2.2			保管方法	○		0	媒体による保管	遠隔地にリモートバックアップすることを推奨する。 [+] コストと実現性を確認した上で、可用性を高めたい場合	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、	媒体による保管	により、データ・プログラムを保管する場所を設置すること。
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	○		0	特定ユーザのみ	部門内利用などでユーザが特定できる場合を想定。 [+] ユーザを特定できない場合	情報システムの利用者数は、	特定ユーザのみ	とする。（●●●●人程度）。
B.1.1.2			同時アクセス数	○		0	特定利用者の限られたアクセス※のみ	登録ユーザから想定する。	情報システムの同時アクセス数は、	特定利用者の限られたアクセス※のみ	とする。（●●●●人程度）。
B.1.1.3			データ量（項目・件数）	○		0	すべてのデータ量が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のデータ量が把握できていない場合	情報システムは、	すべてのデータ量が明確である	（●●●●件程度）。
B.1.1.4			オンラインリクエスト件数※	○		0	処理ごとにリクエスト件数※が明確である	要件定義時には明確にしておく必要がある。 [+] 全部のオンラインリクエスト件数※が把握できていない場合	システムは、	処理ごとにリクエスト件数※が明確である	データ量の詳細は別添に記載のとおりとする。※データ量が明確である場合に記載
B.1.1.5			バッチ処理件数	○		0	処理単位ごとに処理件数が決まっている	要件定義時には明確にしておく必要がある。 [+] 全部のバッチ処理件数が把握できていない場合	情報システムの業務処理件数は、	処理単位ごとに処理件数が決まっている	処理ごとのリクエスト件数の詳細は別添に記載のとおりとする。※リクエスト件数が明確である場合に記載
B.1.2.1			ユーザ数増大率	△		0	1倍	ユーザの登録・削除などのサイクルを確認する。また、将来の見通しについても確認する。 [+] 利用者の増加が見込まれる場合	情報システムのバッチ処理件数は、	1倍	とすること。
B.1.2.2			同時アクセス※数増大率	△		0	1倍	情報システムのピークモデル※がユーザ数の増によってどのように変わると考えているかを確認する。 [+] 利用者の増加が見込まれる場合	情報システムは現状の同時アクセス数から、	1倍	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
B.1.2.3			データ量増大率	△		0	1倍	業務のトレンドによって情報システムで扱うデータ量がどの程度増加するかを確認する。 [+] 段階的稼働や、マスター蓄積システムの場合	情報システムは現状のデータ量から、	1倍	とすること。
B.1.2.4			オンラインリクエスト件数※増大率	△		0	1倍	情報システムの制約となるリクエスト数※の見通しを確認する。	情報システムは現状のオンラインリクエスト件数から、	1倍	とすること。
B.1.2.5			バッチ処理件数増大率	△		0	1倍	情報システムの制約となる処理件数を確認する。	情報システムは現状のバッチ処理件数から、	1倍	とすること。
B.1.3.1			保管期間	△		1	1年	税制などの対応で保管期間が規定されているという想定。 [-] 参照期間が限られていて、バックアップ媒体に吸い上げることが可能な場合 [+] ディスク容量に余裕がある場合	バックアップデータの保管期限は、	1年	とする。
B.2.1.4		性能目標値	通常時オンラインレスポンスタイム※	○	○	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	通常業務時のオンラインレスポンスタイムは、	規定しない	。
B.2.1.5			アクセス集中時のオンラインレスポンスタイム※	○	○	0	規定しない	データの更新頻度が少ない場合。または多い場合でもユーザに対する利用制限などが可能な場合を想定。 [+] 性能低下が、情報システムの評価低下につながる場合	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、	規定しない	。
B.2.2.1			通常時バッチレスポンス※順守度合い	○	○	0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	通常時のバッチレスポンスタイムは、	順守度合いを定めない	こと。
B.2.2.2			アクセス※集中時のバッチレスポンス※順守度合い	○	○	0	順守度合いを定めない	比較的小規模のデータしかないため、バッチのレスポンス順守度に関しては特に規定しないと想定。	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、	順守度合いを定めない	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	○		1	定時内での利用 （1日8時間程度利用）	主に、開庁時間内での利用を想定 [−] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、または24時間利用の場合	情報システムの平日運用時間は、	定時内での利用 （1日8時間程度利用）	を前提とすること。
C.1.1.2			運用時間（休日等）	○		0	規定無し（原則利用しない）	週末は原則利用しないことを想定 [+] 休日出勤する職員の業務に必要なため、休日等も利用する場合	情報システムの休日運用時間は、	規定無し（原則利用しない）	を前提とすること。
C.1.2.2			外部データの利用可否	○		1	一部のデータ復旧に利用できる	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。 [−] 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらからデータを持ってきてシステムを復旧できるような場合	データ復旧の際、外部データの利用は、	一部のデータ復旧に利用できる	こと。
C.1.2.3			データ復旧の対応範囲	○		1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [−] 障害時に発生したデータ損失を復旧する必要がない場合 [+] 職員の作業ミスなどによって発生したデータ損失についても回復できることを保証したい場合	データ復旧の対応範囲は、	障害発生時のデータ損失防止	とすること。
C.1.2.4			バックアップ自動化の範囲	−		2	1ステップのみ手動で行う（外部媒体交換のみ）	バックアップに関するオペレーション※はバックアップ管理のソフトウェアを導入して自動化するが、ハードウェアが対応していないためメディア管理（外部媒体交換）だけは手動にて実施する必要がある。 [−] 手間は増えるが、障害発生時の影響範囲を少なくするため、複数の作業単位に区切ってスクリプト※化する場合 [+] メディア管理も自動で行いたい場合	バックアップは、	1ステップのみ手動で行う（外部媒体交換のみ）	こと。
C.1.2.5			バックアップ取得間隔	○		1	システム構成の変更時など、任意のタイミング	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	バックアップの取得間隔は、	システム構成の変更時など、任意のタイミング	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.1.3.1			監視情報	○		2	エラー監視を行う	災害に備え、遠隔地に用意したハードウェアを使用し、規模を縮小したシステム構成をあらかじめ構築 [+] コストと実現性を確認した上で、可用性を高めたい場合	情報システムの監視については、	エラー監視を行う	こと。
C.2.3.5		保守運用	OS等パッチ※適用タイミング	○	○	4	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [−]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。	OS等のパッチについては、	緊急性の高いパッチ※は即時に適用し、それ以外は定期保守時に適用を行う	ことを目標とする。
C.3.3.1		障害時運用	対応可能時間	−		0	ベンダーの営業時間内（例：9時～17時）で対応を行う	[+]対応が必要な場合	システム異常検知時は、	ベンダーの営業時間内（例：9時～17時）で対応を行う	こと。
C.3.3.2			駆けつけ到着時間	−	○	3	保守員到着が異常検知からユーザの翌営業開始時まで	[+]対応が必要な場合 [−]地理的条件・コスト等により、制限が有る場合。	システム異常時の駆けつけ到着時間は、	保守員到着が異常検知からユーザの翌営業開始時まで	を目標とすること。
C.3.3.4			障害検知通知時間		○	0	障害を検知しない	常駐保守または、サーバをデータセンター※に設置した場合には必要となる。 [+]対応が必要な場合		障害を検知しない	ため、利用者へ連絡は必要ない。
C.4.1.1		運用環境	開発用環境の設置有無	△		0	情報システムの開発用環境を設置しない	ベンダーの開発用環境（案件専用でない）による開発を想定。 [+] 庁舎内に開発用環境を設置した方が開発の効率が良いため短期間で大規模の開発を実施する場合や、セキュリティ上庁舎外にて開発することが難しいソフトウェアの場合		情報システムの開発用環境を設置しない	こと。
C.4.2.1			試験用環境の設置有無	△		2	専用の試験用環境を設置する	専用の試験用環境を設置する。 [−] 開発環境と試験用環境を併用する場合、または、情報システムの試験環境を設置しない場合	情報システムの試験用環境については、	専用の試験用環境を設置する	こと。
C.4.3.1			マニュアル準備レベル	○		0	各製品標準のマニュアルを利用する	情報システムの操作方法について、管理者が製品マニュアルを参照して習得することを想定。必要に応じて、ユーザが運用マニュアルを作成する。 [+] ベンダーよりマニュアルの提供を受ける必要がある場合	運用マニュアルについては、	各製品標準のマニュアルを利用する	こと。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.4.4.1		リモートオペレーション※	リモート監視※地点	－		0	リモート監視※を行わない	庁内LANの範囲内でのみリモート監視を行い、外部（ベンダー拠点等）からの監視を行わない。 [－] サーバ機器についてもコンソールでの直接監視を行う場合 [+]外部（ベンダー拠点等）からの監視を行う場合	情報システムの監視形態は、	リモート監視※を行わない	こと。
C.4.4.3			リモート操作※時の接続方法	－		0	リモート操作※を行わない	仕様の対象としない	情報システムは、	リモート操作※を行わない	こと。
C.4.5.1		運用環境	外部システムとの接続有無	○		0	外部システムと接続しない	部門内システムであり、連携する他システムが存在しない。 [+]連携する他システムが存在する場合		外部システムと接続しない	こと。
C.5.1.2		サポート体制	保守契約（ハードウェア）の種類	－		4	定額保守（オンサイト※）	オンサイトの定額保守が地方公共団体の標準と想定。 [－] 故障時には、公共団体職員が予備機に切り替えることで対処し、保守費を軽減したい場合	ハードウェア保守については、	定額保守（オンサイト※）	とすること。
C.5.2.2			保守契約（ソフトウェア）の種類	○		1	問い合わせ対応	情報システムを構成する個々のソフトウェア製品を調達し、SIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	情報システムのソフトウェア保守契約種類は、	問い合わせ対応	をベンダーが実施すること。
C.5.3.1			ライフサイクル期間	△		1	5年	導入するハードウェア・ソフトウェアのサポート期間に合わせて情報システムのライフサイクルを5年と決定したと想定。 [－] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 情報システムで実行する業務を5年を超えて継続しなければならないため、それにライフサイクルを合わせる場合	情報システムのライフサイクル期間は、	5年	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
C.5.5.1			一次対応役割分担	－		2	すべてベンダーが実施	[−]ユーザにて一次切り分けが実施できるスキルが有る場合	一次対応については、	すべてベンダーが実施	とすること。
C.5.6.2			ベンダ側対応時間帯	－		1	ベンダーの定時時間内（9～17時）	[＋]運用時間帯に合わせて拡張する必要性がある場合 [−]保守契約をしない場合	一次対応における対応時間は、	ベンダーの定時時間内（9～17時）	とすること。
C.5.9.1			定期報告会実施頻度	○	○	3	四半期に1回	[−] 報告の必要が無い場合。 [+] 運用業務委託をしている場合や、SLAを設定している場合、必要に応じて。	運用の定期報告は、	四半期に1回	程度実施すること。
C.5.9.2			報告内容のレベル	○		1	障害報告のみ	[+] 運用業務委託をしている場合や、SLA※を設定している場合、必要に応じて。	保守の定期報告は、	障害報告のみ	実施すること。
C.6.2.1		その他の運用管理方針	問い合わせ対応窓口の設置有無	○		1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定 [−]問い合わせ対応窓口設置しない場合 [+] 常駐するベンダー作業員が問い合わせ対応窓口となる場合等	運用保守時の問い合わせ窓口については、	ベンダーの既設コールセンターを利用する	こと。
D.1.1.1	移行性	移行時期	システム移行期間	○		1	3ヶ月未満	年度を跨いで移行を進める必要がある。 [−] 期間短縮の場合 [+] さらに長期期間が必要な場合	既存システムから新システムへの移行期間は、	3ヶ月未満	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
D.1.1.2			システム停止可能日時	○		1	5日以上	業務への影響が少なく数日以上はシステム停止可能。 [−] さらに停止を多くする場合 [+] 停止を少なくする場合	システム移行時のシステム停止可能日時は、	5日以上	とすること。
D.1.1.3			並行稼働の有無	○		0	無し	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。 [−] 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合	システム移行時の並行稼働期間は、	無し	とすること。
D.3.1.1		移行対象（機器）	設備・機器の移行内容	○		0	移行対象無し	設備機器を新設する必要がある。 [+] 既存設備機器が存在する場合	現行システムで利用している設備・機器は、	移行対象無し	とする。
D.4.1.1		移行対象（データ）	移行データ量	○		1	1TB未満	1TB（テラバイト）未満のデータ（マスター等）を移行する必要がある。 [+] 1TB以上の場合	現行システムから新システムへ	1TB未満	のデータを移行すること。
D.5.1.1		移行計画	移行のユーザ/ベンダ作業分担	○		1	ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 移行データの確認を自治体が実施しない場合	現行システムから新システムへのデータ移行作業は、	ユーザとベンダーと共同で実施	すること。
E.1.1.1	セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	○	○	1	有り	セキュリティポリシー等を順守する必要があることを想定。 [−] 順守すべき規程やルール、法令、ガイドライン等が無い場合	遵守すべき規程、ルール、法令、ガイドライン等は、	有り	とする。（●●●●）

Copyright © 2010−2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.2.1.1		セキュリティリスク分析	リスク分析範囲	○		0	分析なし	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [−] 重要情報の漏洩等の脅威が存在しない（あるいは許容する）場合 [+] 情報の移動や状態の変化が大きい場合	システム開発実施において、セキュリティリスクの	分析なし	とすること。
E.3.1.2		セキュリティ診断	Web診断実施の有無	○		1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。 [−] 内部犯を想定する必要がない場合、Webアプリケーション※を用いない場合	情報システムのWeb診断は、	実施	すること。
E.4.3.4		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	○	○	2	定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。 [−]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	システム脆弱性等に対応するためのウィルス定義ファイルについては、	定義ファイルリリース時に実施	すること。
E.5.1.1		アクセス※・利用制限	管理権限を持つ主体の認証	○		1	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。 [+] 管理権限で実行可能な処理の中に、業務上重要な処理が含まれている場合	情報システムの認証方法は、	1回	とすること。
E.5.2.1			システム上の対策における操作制限度	○		1	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	不正なソフトウェアがインストールされる、不要なアクセス※経路（ポート※等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス※方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある） [−] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策で対処する場合	情報システムへの操作制限は、	必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可	すること。
E.6.1.1		データの秘匿	伝送データの暗号化の有無	○		1	認証情報のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+] 外部ネットワークと接続する場合	伝送データについては、	認証情報のみ暗号化	すること。

Copyright © 2010−2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
E.6.1.2			蓄積データの暗号化の有無	○		1	認証情報のみ暗号化	蓄積するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [+]物理記録媒体の盗難・紛失の可能性が有る場合	蓄積データについては、	認証情報のみ暗号化	すること。
E.7.1.1		不正追跡・監視	ログ※の取得	○		1	必要なログを取得する	不正なアクセス※が発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログ※を取得する必要がある。 （ログ※取得の処理を実行することにより、性能に影響する可能性がある）	ログの取得については	必要なログを取得する	こと。
E.7.1.3			不正監視対象（装置）	○		1	重要度が高い資産を扱う範囲、あるいは、外接部分	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ※等の範囲を定めておく必要がある。	不正監視対象は、	重要度が高い資産を扱う範囲、あるいは、外接部分	とすること。
E.10.1.1		Web対策	セキュアコーディング※、Webサーバ※の設定等による対策の強化	○		1	対策の強化	オープン系のシステムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバ※に対する対策を実施する必要がある。 [−] Webアプリケーション※を用いない場合	セキュアコーディング、Webサーバの設定等は、	対策の強化	すること。
E.10.1.2			WAF※の導入の有無	○		0	無し	内部ネットワークのみ接続する情報システムを想定、そのため、ネットワーク経由での攻撃に対する脅威が発生する可能性は低い。 [+] 外部ネットワークと接続する場合	WAFの導入は、	無し	とすること。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	○		0	制約無し	特に制限などを受けない場合を想定。 [+] 法や条例の制約を受ける場合、もしくは業界などの標準や取り決めなどがある場合	システム構築時には、条例等の	制約無し	とすること。

Copyright © 2010-2014 IPA, LASDEC

項番	大項目	中項目	メトリクス（指標）	クラウド調達時の扱い	検収時の扱い	各要求事項シートで選択したレベル			情報システム調達仕様書記載例		
						選択レベル		選択時の条件			
F.1.2.1			運用時の制約条件	○		0	制約無し	特に制限などを受けない場合を想定。 [+] 設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	システム運用時には、	制約無し	とすること。
F.2.2.1		システム特性	クライアント※数	△		0	特定クライアント※のみ	特定のクライアントのみが使用することを想定。 [+] 将来的にクライアント数の増加が予想され、上限値で合意が必要な場合	情報システムで利用するクライアント数は、	特定クライアント※のみ	とすること。（●●●●人程度）。
F.2.5.1			特定製品の採用有無	－		0	特定製品の指定がない	構成する機器に関して指定製品がない場合を想定。 [+] 特に指定があった場合	情報システムでは、	特定製品の指定がない	。
F.3.1.1		適合規格	規格取得の有無(安全性)	－		0	規格取得の必要無し	機器の規格取得に関して指定がない場合を想定。 [+] 特に指定があった場合	情報システムはUL60950等の	規格取得の必要無し	とする。
F.3.2.1			規格取得の有無（有害物質）	△		0	規格取得の必要無し	特に制限などを受けない場合を想定。 [+] 特に指定があった場合	情報システムでは、	規格取得の必要無し	とする。
F.5.1.1		環境マネージメント	グリーン購入法対応度	－		0	対処不要	団体の方針によるものと想定。 [+]団体の方針による。	情報システムのグリーン購入法については、	対処不要	とする。

Copyright © 2010-2014 IPA, LASDEC

地方公共団体の情報システム調達仕様書における非機能要件の標準化に関する調査研究

平成２６年３月発行
発行　財団法人　地方自治情報センター
〒102-8419 東京都千代田区一番町２５番地（全国町村議員会館内）
電話０３（５２１４）８００２

－禁無断転載－

LASDEC（ラスデック）、当センターの組織名の英語表記（Local Authorities Systems Development Center）を略したものです。

LASDEC