
非機能要求グレード2018

システム基盤の非機能要求に関するグレード表

2018年4月

非機能要求グレード 2018
システム基盤の非機能要求に関するグレード表
2018年4月

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター
(c)2010-2018 独立行政法人情報処理推進機構

[使用条件]

1. 本資料の著作権は、独立行政法人情報処理推進機構が保有しています。
2. 本資料は著作権法による保護を受けており、本資料の利用者は、本資料の全部または一部を項番3に定める場合を除き、独立行政法人情報処理推進機構の許諾なく無断で改変、公衆送信、販売、出版、翻訳/翻案することは営利目的、非営利目的に関わらず禁じられています。
3. 独立行政法人情報処理推進機構は、本資料の利用者が、以下の著作権表示を明記することを条件として、①及び②の行為を行うことを許諾します。
著作権表示:(c)2010-2018 独立行政法人情報処理推進機構
①本資料の全部または一部を複製すること。
②本ページに記載されている使用条件を配布先に遵守させることを条件に本資料の複製物を無償で再配布すること。
4. 独立行政法人情報処理推進機構は、本資料が第三者の著作権、特許権、実用新案権等の知的財産権に抵触しないことを一切保証するものではなく、また、本資料の内容に誤りがあった場合でも一切責任を負いかねます。
5. 独立行政法人情報処理推進機構は、本ページで記載された許諾内容を除き、独立行政法人情報処理推進機構または第三者の著作権、特許権、実用新案権等の知的財産権に基づくいかなる権利を許諾するものではありません。
6. 独立行政法人情報処理推進機構は、本資料のシステム開発への利用、開発されたシステムの使用、及び当該システムの使用不能等により生じるいかなる損害についても、なんら責任を負うものではありません。
7. 本資料を海外へ持ち出す場合及び非居住者に提供する場合には、「外国為替及び外国貿易法」の規制及び米国輸出管理規則等外国の輸出関連法規を確認のうえ、必要な手続きを行って下さい。
8. 本資料へのお問い合わせについては、独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センターまでご連絡下さい。

・モデルシステムシートの凡例

項番	大項目	特徴	社会的影響が殆ど無いシステム	社会的影響が限定されるシステム	社会的影響が極めて大きいシステム
モデルシステムイメージ					
モデルシステムの概要			企業の特定部門が比較的限られた範囲で利用しているシステムで、機能が低下または利用不可な状態になった場合、利用部門では大きな影響があるが、その他には影響しないもの。 ここでは、ごく小規模のインターネット公開システムを想定している。	企業活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、当該企業活動に多大の影響を及ぼすと共に取引先や顧客等の外部利用者にも影響を及ぼすもの。 ここでは、企業内のネットワークに限定した基幹システムを想定している。	国民生活・社会経済活動の基盤となるシステムで、その機能が低下又は利用不可能な状態に陥った場合、国民生活・社会経済活動に多大な影響を与えるもの。 ここでは、不特定多数の人が利用するインフラシステムを想定している。
1	可用性	稼働率	・1年間で数日程度の停止まで許容できる(稼働率99%)。	・1年間で1時間程度の停止まで許容できる(稼働率99.99%)。	・1年間で数分間程度の停止まで許容できる(稼働率99.999%)。
2		目標復旧水準	・データのリカバリを伴う復旧では、週次のバックアップからの復旧が目標水準となる。	・データのリカバリを伴う復旧では、1営業日以内での復旧が目標水準となる。	・データのリカバリを伴う復旧では、数時間で障害発生時点までの復旧が目標水準となる。
3		大規模災害	・大規模災害時は、システムの再構築による復旧が前提となる。	・大規模災害時は1週間以内での復旧を目指す。	・大規模災害時はDRサイトでの業務継続性が要求される。 ・バックアップセンターを設置し、大規模災害に備える。

(a) (b) (c)

(a) 項番 : 特徴の連番。

(d)

(b) 大項目 : 特徴のカテゴリ。非機能要求グレードの大項目と同じ。

(c) 特徴 : モデルシステム毎に想定される非機能要求の特徴。モデルシステム名称だけでは非機能要求レベルがわかりにくいいため、モデルシステムの特徴を表すよう抽出した。

(d) モデルシステム : 実現するシステムの参考となる典型的な非機能要求モデル。独立行政法人情報処理推進機構(IPA)が公開している重要インフラ情報システム信頼性研究会のシステムプロファイリングから3つの名称を引用し、それぞれの特徴を定義した。
(重要インフラ情報システム信頼性研究会報告書の公開について URL <https://www.ipa.go.jp/sec/softwareengineering/reports/20090409.html>)

・グレード表の凡例

項番	大項目	中項目	小項目	小項目説明	重要項目	マトリクス (指標)	レベル						運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム			
							0	1	2	3	4	5			選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件		
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	○	運用時間(通常)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度 の停止有り (9時～翌朝8時)	若干の停止 有り (9時～翌朝8時55分)	24時間無 停止	【重複項目】 C.1.1.1。運用時間は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【マトリクス】 運用時間は、オンライン/バッチを含みシステムが稼働している時間帯を指す。 【レベル】 ①内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。「規定なし」は、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している(例:障害発生に備えた予備システム、開発・検証用システム等)。「定時内」や「夜間のみ」は、一般的な業務形態を想定したもので、業務が稼働する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。「停止あり」とは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。「24時間無停止」は、オンライン業務が稼働していない時間にバッチを稼働させる必要があり、システムを停止することができないようなケースも含まれる。	2	夜間のみ 停止 (9時～21時)	夜間を実施する業務はなく、システムを停止可能。 [-] 運用時間をもとに限って業務を稼働させる場合 [+] 24時間無停止やリポート処理等の短時間の停止のみを考える場合	4	若干の停止 有り (9時～翌朝8時55分)	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [-] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無 停止	システムを停止できる時間帯が存在しない。 [-] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
A.1.1.2					○	運用時間(特定日)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度 の停止有り (9時～翌朝8時)	若干の停止 有り (9時～翌朝8時55分)	24時間無 停止	【重複項目】 C.1.1.2。運用時間は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【マトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある(例:「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリポートをするためその日はレベル3」など)。また、「ユーザの休日」だけでなく、「ベンダの休日」についても特定日として認識し、運用保守体制等を整合すること。	0	規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日/バックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ 停止 (9時～21時)	週末はバックアップ運用のための、夜間は停止する。 [-] 週末運用するバックアップやバッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日も運用する場合	5	24時間無 停止	システムを停止できる時間帯が存在しない。 [-] 定期的に運用を停止する日が存在する場合
A.1.1.3					○	計画停止の有無	計画停止 有り(運用 スケジュール の変更可)	計画停止 有り(運用 スケジュール の変更不可)	計画停止 無し				【重複項目】 C.2.1.1。計画停止の有無は、システムの可用性の実現レベルを表す項目であるとともに、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【運用コストへの影響】 計画停止が「有り」の場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。	0	計画停止 有り(運用 スケジュール の変更可)	事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止 有り(運用 スケジュール の変更不可)	24時間無停止での運用は必要ない。停止可能な時間が存在し、計画的な停止は可能。 [-] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止 無し	システムを停止できる時間帯が存在しない。 [-] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合

← 項目定義 → (a) (b) (a) (b) (a) (b)

グレード表のモデルシステムに関する記述よりも左側の列は、重要項目列の有無を除いて、項目一覧と同様であるので、項目一覧の凡例を参照のこと。

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

(b) 選択時の条件 : ベース値を選択した時の条件。ベース値だけでは実現するシステムの非機能要求を適切に提示できない場合を想定し、ベース値を変更する場合の条件を[-][+]で示した。
対象システムの非機能要求レベルを下げたい場合は[-]に書かれている条件を確認し、逆に非機能要求レベルを上げたい場合は[+]に書かれている条件を確認の上レベル調整を行う。

モデルシステムシート

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

注: モデルシステムの名称は、独立行政法人情報処理推進機構(IPA)が公開している重要インフラ情報システム信頼性研究会のシステムプロファイリングから引用した。
重要インフラ情報システム信頼性研究会報告書の公開について URL <https://www.ipa.go.jp/sec/softwareengineering/reports/20090409.html>
「重要インフラ情報システム信頼性研究会」のシステムプロファイリングではシステムのカテゴリが4つ存在するが、非機能要求グレードにおけるモデルシステムでは経済損失レベルや公共的影響有りといった影響度合を考慮し、「人命への影響、甚大な経済損失が予想されるシステム」については「社会的影響が極めて大きいシステム」の中に含めている。

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム					
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件			
A.1.1.1	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	○	運用時間(通常)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の 停止有り (9時～翌朝8時)	若干の停止有り (9時～翌朝8時55分)	24時間無停止	○	【重複項目】 C.1.1.1. 運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【マトリクス】 運用時間は、オンライン/パッチを含みシステムが稼働している時間帯を指す。 【レベル】 ①内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している(例:障害発生に備えた予備システム、開発・検証用システム等)。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼働していない時間にパッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。	2	夜間のみ 停止 (9時～21時)	夜間に実施する業務はなく、システムを停止可能。 [-] 運用時間をもっと限って業務を稼働させる場合 [+] 24時間無停止やリポート処理等の短時間の停止のみを考える場合	4	若干の停止有り (9時～翌朝8時55分)	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [-] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [-] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
A.1.1.2			運用時間(特定日)	規定無し		定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の 停止有り (9時～翌朝8時)	若干の停止有り (9時～翌朝8時55分)	24時間無停止	【重複項目】 C.1.1.2. 運用時間は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【マトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある(例:「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリポートをするためその日はレベル3」など)。また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。	0		規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日にバックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ 停止 (9時～21時)	週末はバックアップ運用のみのため、夜間は停止する。 [-] 週末運用するバックアップやパッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日も運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [-] 定期的に運用を停止する日が存在する場合		
A.1.1.3			計画停止の有無	計画停止有り(運用スケジュールの変更可)		計画停止有り(運用スケジュールの変更不可)	計画停止無し				【重複項目】 C.2.1.1. 計画停止の有無は、システムの可用性の実現レベルを表す項目であると共に、運用・保守性に関する開発コストや運用コストを検討する上でも必要となる項目であるため、可用性と運用・保守性の両方に含まれている。 【運用コストへの影響】 計画停止が"有り"の場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。	0		計画停止有り(運用スケジュールの変更可)	事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止有り(運用スケジュールの変更不可)	24時間無停止での運用は必要ない。停止可能な時間が存在し、計画的な停止は可能。 [-] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止無し	システムを停止できる時間帯が存在しない。 [-] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合		
A.1.2.1			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。	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	全ての業務	【マトリクス】 ここでの対象業務範囲とは、稼働率を算出する際の対象範囲を指す。 【レベル】 内部向けとは対象とするシステム内に閉じた処理(業務)、外部向けとは他システムとの連携が必要な処理(業務)を表している。	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。 [+] 外部向け業務も実施しており、必要な業務としている場合	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。 [-] 外部との業務が必要ない場合 [+] 業務継続に、外部とのリアルタイムでの処理が必要な場合	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。 [-] 業務継続に、外部とのリアルタイムでの処理が必要とならない場合		
A.1.2.2					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	○	【マトリクス】 サービス切替時間とは、想定できる障害(例えばハードウェアの故障等)により業務が一時的に中断するケースなど)に対して、対策を施すこと(例えばクラスタ構成でのサーバの切替えなど)により、業務再開までに要する時間を指す。 【運用コストへの影響】 中断を許容する時間が長くなれば、復旧対策としてはシステムでの自動化から人員による手動での対処に比重が移るため、運用コストへの影響が出てくる。	1	24時間未満	外部向けの業務はなく、1日程度で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	
A.1.2.3					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					【マトリクス】 業務継続の要求度とは、発生する障害に対して、どこまで業務を継続させる必要があるかを示す考え方の尺度を示している。システムを構成する機器や部位には、単一障害点SPOF(Single Point Of Failure)が多数存在し、システム停止となるリスクを多く含んでいる。これらのSPOFを許容するか、冗長化などの対策で継続性をどこまで確保するかが要求の分かれ目となる。	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。	
A.1.3.1			目標復旧水準(業務停止時)	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。	RPO(目標復旧地点)	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)				【マトリクス】 RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。 【レベル3】 障害発生時点とは、障害が発生する直前のトランザクションなどの処理が完了している時点のことを指し、障害発生時点まで復旧するためには、発生直前の完了した処理のジャーナルログが保証されていることが前提となる。またジャーナルログをアーカイブすることで、障害発生までの任意の時点への復旧に対応することを想定している。	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、データ損失の影響が大きい場合	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)	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。	
A.1.3.2					RTO(目標復旧時間)	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			【マトリクス】 サービス切替時間(A.1.2.2)での復旧時間と異なり、RTOでの復旧時間は、業務の継続対策を実施していない(業務停止となる)ケースでの障害での復旧時間を指している。RLOで業務の復旧までを指定している場合、該当する業務のデータの復旧までが対象であり、業務再開の整合性の確認は別途必要となる。	1	1営業日以内	目標復旧地点を考慮し、システムの規模から判断する。 [-] 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	2	12時間以内	目標復旧地点を考慮し、システムの規模から判断する。 [-] 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	4	2時間以内	なるべく早く復旧する。	
A.1.3.3					RLO(目標復旧レベル)	システムの復旧	特定業務のみ	全ての業務					【マトリクス】 業務停止を伴う障害が発生した際、何を復旧の対象とするかのレベルを示す。 【レベル0】 システムの復旧は、ハードウェアの復旧だけでなくデータのリストアまでを対象とする。 【レベル1】 特定業務とは、例えばA.1.2.1対象業務範囲で定義する継続性が要求される業務などを指す。	1	特定業務のみ	主要な業務のみを対象とすることができ。 [+] 業務毎に影響を切り離せない場合	2	全ての業務	全ての業務が稼働していないと影響がある。 [-] 影響を切り離せる業務がある場合	2	全ての業務	全ての業務が稼働していないと影響がある。 [-] 影響を切り離せる業務がある場合	

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル						運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム	
							0	1	2	3	4	5			選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件
A.1.4.1			目標復旧水準 (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、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。		システム再開目標	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		【マトリクス】 大規模災害としては、RPO、RTO、RLOなどの細かな要求までは確定せず、システム再開目標として大まかな復旧時間を設定する。目標復旧レベルについては、業務停止時の目標復旧水準を参考とする。	1	数ヶ月以内に再開 [-] データを持たず、復旧が不要な場合 [+] 業務停止の影響が大きい場合	3	一週間以内に再開 [-] 代替機器の調達や、復旧体制の準備に時間がかかる場合 [+] 業務停止の影響が大きく、DRサイトによる早急な復旧が必要な場合	4	3日以内に再開 [+] 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
A.1.5.1			稼働率	明示された利用条件の下で、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。		稼働率	95%以下	95%	99%	99.9%	99.99%	99.999%		【レベル】 24時間365日の稼働の場合、1年間で業務が中断する時間の合計は、それぞれ以下の通りとなる。 95%.....18.3日 99%.....87.6時間 99.9%..... 8.76時間 99.99%..... 52.6分 99.999%..... 5.26分 また1日8時間で週5日稼働のシステムではサービス切替時間と稼働率の関係は以下の通りとなる。 週に1時間....97.5% 月に1時間....99.4% 年に1時間....99.95%	2	99% 1年間で数時間程度の停止を許容。 備考に記載した稼働率での目安となる稼働時間を参考にして決定する。	4	99.99% 1年間で1時間程度の停止を許容。	5	99.999% 1年間で数分程度の停止までしか許容できない。
A.4.2.1		回復性	可用性確認	可用性として要求された項目をどこまで確認するかの範囲。		確認範囲	実施しない。または単純な障害の範囲	業務を継続できる障害の範囲	業務停止となる障害のうち一部の範囲	業務停止となる障害の全ての範囲				【レベル】 レベル2および3の確認範囲には、レベル1で定義した内容を含む。	1	業務を継続できる障害の範囲 [-] 障害時の対策を考慮しない場合 [+] 業務停止となる障害が発生した際、その復旧方法を事前に確認しておく必要がある場合	2	業務停止となる障害のうち一部の範囲 業務停止となる障害に対しての対策を確立する必要があるが、リスクの高い障害や、障害の種類により確認を限定することが可能な場合。 [-] 業務停止となる障害による影響が極めて少ないと判断できる場合 [+] 障害の種類や発生リスクを考慮せず、可能な範囲で確認が必要な場合	3	業務停止となる障害の全ての範囲 業務停止による影響が極めて大きく、考えられる障害に対して事前に確認が必要となる場合。 [-] 障害の種類や発生リスクにより、システムへの影響を限定できる場合
B.1.1.1	性能・拡張性	業務処理量	通常時の業務量	性能・拡張性に影響を与える業務量。 該当システムの稼働時を想定し、合意する。 それぞれのマトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	○	ユーザ数	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					【重複項目】 F.2.1.1。ユーザ数は性能・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ため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。	0	特定ユーザのみ [+] ユーザを特定できない場合	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	2	不特定多数のユーザが利用 国民全体がアクセスする可能性があるような場合を想定。 [-] 一定の上限値を設定することが可能な場合
B.1.1.2						同時アクセス数	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					【マトリクス】 同時アクセス数とは、ある時点でシステムにアクセスしているユーザ数のことである。	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。 [+] ユーザを特定できない場合	1	同時アクセスの上限が決まっている 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。	2	不特定多数のアクセス有り 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。
B.1.1.3						データ量	全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、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、マスター系テーブルや主なトランザクションデータの一次保存分などがある。 主要なデータ量しか決まっていない場合、後工程に於いて、検討漏れデータの出現などによるディスク追加などが発生するリスクがある。	0	全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	0	全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	0	全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
B.1.1.4						オンラインリクエスト件数	処理毎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						【マトリクス】 オンラインリクエスト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・転出処理やネットショッピングシステムの決済処理などがある。 主なリクエスト件数しか決まっていない場合、後工程に於いて、検討漏れリクエストの出現などによるサーバ能力不足などのリスクがある。	0	処理毎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	0	処理毎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	0	処理毎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
B.1.1.5						バッチ処理件数	処理単位毎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						【マトリクス】 バッチ処理件数は単位時間を明らかにして確認する。要件定義時には主な処理(特に該当システムでクリティカルとなる処理)では処理件数のおおよその目安は決まっているはずであり、それを元に性能や拡張性の検討を進める。要件定義時に明確になっていない場合は、確定度も含め、想定しておく。 【レベル1】 主な処理とは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。 主なバッチ処理件数しか決まっていない場合、後工程に於いて、検討漏れ処理の出現などによるサーバ能力不足などのリスクがある。	0	処理単位毎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	0	処理単位毎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	0	処理単位毎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

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル						運用コストへの影響	備考	社会的影響が殆ど無いシステム			社会的影響が限定されるシステム			社会的影響が極めて大きいシステム		
							0	1	2	3	4	5			選択レベル	選択時の条件		選択レベル	選択時の条件		選択レベル	選択時の条件	
B.1.2.1			業務量増大度	システム稼働開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率。 必要に応じ、開始日の平均値や、開始後の定常状態との比較を行う場合もある。		ユーザ数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	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	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	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
B.1.2.2						同時アクセス数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	1倍	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	1	1.2倍	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リンクしない場合 [+] 利用者の増加が見込まれる場合	1	1.2倍	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リンクしない場合 [+] 利用者の増加が見込まれる場合
B.1.2.3						データ量増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	1倍	業務のトレンドによって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	1	1.2倍	業務のトレンドによって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 [+] 段階的稼働や、マスター蓄積システムの場合	1	1.2倍	業務のトレンドによって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 [+] 段階的稼働や、マスター蓄積システムの場合
B.1.2.4						オンラインリクエスト件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【マトリクス】 オンラインリクエスト件数は単位時間を明らかにして確認する。 【レベル】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	1倍	システムの制約となるリクエスト数の見直しを確認する。	1	1.2倍	システムの制約となるリクエスト数の見直しを確認する。	1	1.2倍	システムの制約となるリクエスト数の見直しを確認する。
B.1.2.5						バッチ処理件数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【マトリクス】 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】 レベルに示した倍率はおおまかな目安を示しており、具体的には数値で合意する必要がある。	0	1倍	システムの制約となる処理件数を確認する。	1	1.2倍	システムの制約となる処理件数を確認する。	1	1.2倍	システムの制約となる処理件数を確認する。
B.1.3.1			保管期間	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、データの種別毎に定める。 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。		保管期間	6ヶ月	1年	3年	5年	10年以上 有期	永久保管		【レベル】 対象が複数あり、それぞれ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。 【レベル0】 保管期間の制約が短い場合は6ヶ月で代用する。	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	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	4	10年以上 有期	エンドユーザに保証している外部要件などで、保管期間が決められていると想定。 [-] 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
B.2.1.1		性能目標値	オンラインレスポンス	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ふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎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)		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		【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。	0	順守率を定めない	トランザクションの量が少ない場合。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、システムの評価低下につながる場合	3	90%	管理対象とする処理の中で、通常時のトランザクション数の90%が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、システムの評価低下につながる場合	5	99%以上	管理対象とする処理の中で、通常時のトランザクション数の99%が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
B.2.1.2						ピーク時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上		【レベル】 具体的な目標値や約束値がある場合、各処理の順守率を規定する。 レベルに示した順守率はおおまかな目安を示しており、具体的にはレスポンスと順守率について数値で合意する必要がある。	0	順守率を定めない	トランザクションの量が少ない場合。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、システムの評価低下につながる場合	2	80%	管理対象とする処理の中で、ピーク時のトランザクション数の80%が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、システムの評価低下につながる場合	4	95%	管理対象とする処理の中で、ピーク時のトランザクション数の95%が目標値を達成できれば良いと想定。 [-] 遅くとも、処理出来れば良いか代替手段がある場合 [+] 性能低下が、システムの評価低下につながる場合
B.2.2.1			バッチレスポンス(ターンアラウンドタイム)	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ふまえ、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、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎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)		通常時レスポンス順守度合い	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					【レベル1】 所定の時間には再実行は含まない。	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。	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	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。
B.2.2.2						ピーク時レスポンス順守度合い	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					【レベル1】 所定の時間には再実行は含まない。	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。	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	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

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	メトリクス (指標)	レベル						運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム				
							0	1	2	3	4	5			選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件			
B.3.1.1		リソース拡張性	CPU拡張性	CPUの拡張性を確認するための項目。 CPU利用率は、将来の業務量の増加に備え、どれだけCPUに余裕をもたせておくかを確認するための項目。 CPU拡張性は、物理的もしくは仮想的に、どれだけCPUを拡張できるようにしておくかを確認するための項目。 CPUの専有の有無については「B.4.1 HWリソース専有の有無」で確認する。		CPU利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【メトリクス】 CPU利用率は単位時間に、実行中のプログラムがCPUを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 CPU利用率が大きい場合、少しの業務量増大で機器増設などの対策が必要になる。	0	80%以上	システムが過剰設備となっていないという想定。 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [-] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [-] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合
B.3.1.2				CPU拡張性	1倍 (拡張要求なし)	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能			○	【運用コストへの影響】 CPU拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。	0	1倍 (拡張要求なし)	部門内限定の利用であり、CPUの拡張が不要な場合	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、CPU増設を可能にしたと想定。	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、CPU増設を可能にしたと想定。	
B.3.2.1		メモリ拡張性	メモリの拡張性を確認するための項目。 メモリ利用率は、将来の業務量の増加に備え、どれだけメモリに余裕をもたせておくかを確認するための項目。 メモリ拡張性は、物理的もしくは仮想的に、どれだけメモリを拡張できるようにしておくかを確認するための項目。 メモリの専有の有無については「B.4.1 HWリソース専有の有無」で確認する。		メモリ利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【メトリクス】 メモリ利用率は単位時間に、実行中のプログラムがメモリを使用している割合を示している。単位時間をどの程度にするか、また、動作するプログラムの特性によって数値は大きく異なる。 【レベル】 レベルに示した利用率はおおまかな目安を示しており、具体的な数値で合意する必要がある。 【運用コストへの影響】 メモリ利用率が大きい場合、少しの業務量増大でメモリや機器の増設が必要になる。	0	80%以上	システムが過剰設備となっていないという想定。 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [-] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合	1	50%以上 80%未満	業務量の増加に備え、余裕を持たせている状態を想定。 [-] 性能・拡張性より低コストであることを優先する場合 [+] 近い将来利用者が増える予定がある場合	
B.3.2.2				メモリ拡張性	1倍 (拡張要求なし)	1.5倍の拡張が可能	2倍の拡張が可能	4倍の拡張が可能	8倍以上の拡張が可能			○	【運用コストへの影響】 メモリ拡張性がない場合、機器自体の増設や、環境や契約の変更が必要になる場合がある。	0	1倍 (拡張要求なし)	部門内限定の利用であり、メモリの拡張が不要な場合	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、メモリ増設を可能にしたと想定。	1	1.5倍の拡張が可能	2～3年後のシステム拡張に備え、メモリ増設を可能にしたと想定。	
C.1.1.1	運用・保守性	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼働させ、オンライン処理やバッチ処理を実行している時間帯のこと。	○	運用時間(通常)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の停止有り (9時～翌朝8時)	若干の停止有り (9時～翌朝8時55分)	24時間無停止		【重複項目】 A.1.1.1。運用時間(通常)は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 運用時間は、オンライン/バッチを含みシステムが稼働している時間帯を指す。 【レベル】 ()内の時間は各レベルの一例を示したもので、レベル選定の条件とはしていない。規定無しは、固定のサービス時間が存在しないことを示し、基本的にシステムは停止していて、必要に応じてユーザがシステムを起動するようなケースを想定している(例:障害発生に備えた予備システム、開発・検証用システム等)。定時内や夜間のみ停止は、一般的な業務形態を想定したもので、業務が稼動する時間帯が異なるシステムにおいては、時間帯をスライドさせるなどの読替えが必要である。停止有りとは、システムを停止しなければならない時間帯ではなく、システムを停止できる可能性のある時間帯を指す。24時間無停止は、オンライン業務が稼働していない時間にバッチを稼動させる必要があり、システムを停止することができないようなケースも含まれる。	2	夜間のみ 停止 (9時～21時)	夜間に実施する業務はなく、システムを停止可能。 [-] 運用時間をもっと限って業務を稼働させる場合 [+] 24時間無停止やリポート処理等の短時間の停止のみを考える場合	4	若干の停止有り (9時～翌朝8時55分)	24時間無停止での運用は必要ないが、極力システムの稼働は継続させる。 [-] 夜間のアクセスは認めないなど、長時間運用を停止する場合 [+] 24時間無停止で運用する場合	5	24時間無停止	システムを停止できる時間帯が存在しない。 [-] 1日のスケジュールで定期的に運用を停止する時間帯が存在する場合
C.1.1.2							運用時間(特定日)	規定無し	定時内 (9時～17時)	夜間のみ 停止 (9時～21時)	1時間程度の停止有り (9時～翌朝8時)	若干の停止有り (9時～翌朝8時55分)	24時間無停止		【重複項目】 A.1.1.2。運用時間(特定日)は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【メトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある(例:「月～金」はレベル2だが、土日はレベル0)、「通常」はレベル5だが、毎月1日にリブートをするためその日はレベル3」など)。また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。	0	規定無し	通常と異なる運用時間となる特定日は存在しない。 [+] 休日にバックアップ運用を行うなど、通常とは異なる運用時間となる特定日が存在する場合	2	夜間のみ 停止 (9時～21時)	週末はバックアップ運用のための、夜間は停止する。 [-] 週末運用するバックアップやバッチ処理などが存在せず、土休日は運用を停止する場合 [+] 休日出勤する社員の業務に必要なため、土休日も運用する場合	5	24時間無停止

項番	大項目	中項目	小項目	小項目説明	重複項目	メトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム					
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件			
C.1.2.2			バックアップ	システムが利用するデータのバックアップに関する項目。		外部データの利用可否	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				【メトリクス】 外部データとは、当該システムの範囲外に存在するシステムの保有するデータを指す（開発対象のシステムと連携する既存システムなど）。外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。	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	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、そこ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	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、そこ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	
C.1.2.3						バックアップ利用範囲	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	ユーザーからの回復	データの長期保存（アーカイブ）			【メトリクス】 マルウェア等によるデータ損失への備えや、監査のためのログの退避など、セキュリティ観点のバックアップも考慮すること。 【レベル2】 ユーザーからの回復の場合、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、複数世代のバックアップの管理や時間指定回復（Point in Time Recovery）等の機能が必要となる場合が考えられる。	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 [+] 復旧時点（RPO）が固定ではなく、障害の内容に応じて時間指定で復旧する必要がある場合	2	ユーザーからの回復	管理者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。 [-] 管理者の作業ミスによる復旧は管理者が作業前に個別にデータ保全作業を実施することで担保することとし、バックアップによる回復は必要としない場合 [+] データ損失からの回復だけでなく、過去データの保存用途に用いる場合	3	データの長期保存（アーカイブ）	内部統制対応の要件に基づき、データの履歴を保存する必要がある。 [-] バックアップはデータ損失からの回復に対する用途にのみ使用する場合	
C.1.2.4						バックアップ自動化の範囲	全ステップを手動で行う	一部のステップを手動で行う	全ステップを自動で行う			○	【メトリクス】 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 ・バックアップ先の選択 ・ファイル転送 などといった作業ステップが存在する。 【運用コストへの影響】 バックアップ運用の自動化を実現するためには、ハードウェア・ソフトウェアに対する投資が必要となり導入コストは増大する。しかし、運用中におけるバックアップ作業をユーザが実施する必要がなくなるため、その分運用コストは減少すると考えられる。	0	全ステップを手動で行う	バックアップに関するオペレーションはスケジュール管理も含めて基本的に手動で実行する。 [+] バックアップに関する管理者のオペレーションを削減したい場合	1	一部のステップを手動で行う	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、一部の作業（特定のコマンド実行、テープ交換等）は手動にて実施する必要がある。 [-] 管理者が全てのステップを手動で実行する場合 [+] バックアップ運用の全てのステップを自動で行いたい場合	2	全ステップを自動で行う	バックアップに関するオペレーション（スケジュール管理、メディア管理、ジョブ実行等）に関して、管理ソフトウェアを導入して自動で行うことを想定。 [-] 管理者が手動でバックアップを実行する場合	
C.1.2.5						バックアップ取得間隔	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		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が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が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	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	5	同期バックアップ	RTOの要件を満たすため、更新内容をバックアップサイトへ転送し、障害発生時にすぐに運用が可能なDRサイトを構成することを想定。 [-] 障害発生時にバックアップからのリカバリ作業のため運用の停止が許されるような場合	
C.1.2.6						バックアップ保存期間	バックアップを保存しない	1年未満	3年	5年	10年以上有限	永久保存		【メトリクス】 主に可用性の観点で実施されるバックアップの世代管理とは別に、ここではデータ保全という観点でバックアップデータの保存期間を検討する。	0	バックアップを保存しない	バックアップデータは障害復旧用途にのみ利用されるものであり、データ保存の用途には使用しないことを想定。 [+] バックアップをデータアーカイブの用途に利用するような場合	2	3年	社内規定でデータの更新履歴を3年間保持しなければならないことを想定。 [-] 保管先容量の制限で3年分をシステム上に保持できない場合 [+] 社内外の規定が変更されて保存期間が延長されることが想定される場合	4	10年以上有限	10年間のデータ保存が法律で規定されているような場合を想定。 [-] 保管先容量の制限で10年分をシステム上に保持できない場合 [+] 保管先容量に制限がなく、永続的にデータを保管しなければならない場合

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	メトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム				
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件		
C.1.3.1			運用監視	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。 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。		監視情報	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	○ 【メトリクス】 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。また、監視情報の発報先については、「C.4.5.2 監視システムの有無」で確認すること。 【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I/O、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、システムの品質を維持するための運用コストが下がる。	2	エラー監視を行う	管理者がすぐに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をのみで通知できればよい。 [-] 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	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	4	リソース監視を行う	CPU使用率やスワップの発生状況等に対して閾値を設定し、サービスレベル低下の予兆を監視して、システムの拡張計画や運用スケジュールの検討を行うことを想定。 [-] 障害の発生を検知して管理者への対応を促すのみで良い場合 [+] 業務アプリケーションの応答時間やスループットなど、より厳密にシステムのサービスレベルを評価したいような場合
C.1.3.2				監視間隔		監視を行わない	不定期監視(手動監視)	定期監視(1日間隔)	定期監視(数時間間隔)	リアルタイム監視(分間隔)	リアルタイム監視(秒間隔)		1	不定期監視(手動監視)	必要に応じて管理者が手動確認を行うため、診断間隔は不定期となることを想定。 [+] 手動確認ではなく、システムに監視をさせて必要に応じて管理者に通知をさせたい場合	4	リアルタイム監視(分間隔)	障害を検知するまでの時間がかかってしまうが、システムに対する監視情報収集のコストを低くすることを優先し、分間隔での監視とすることを想定。 [-] 障害の検知はアプリケーションの機能で実装し、システム基盤としての監視としては定期的な運用状況のレポートのみでよいような場合 [+] 障害検知までの時間を短縮したいような場合	5	リアルタイム監視(秒間隔)	障害発生時にはすぐに検知して対処に移れるように、秒間隔での監視を行うことを想定。 [-] 監視情報の収集がアプリケーションのパフォーマンスに影響するリスクを回避するため、監視間隔を広げるような場合	
C.2.1.1		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサービス停止に関する項目。	○	計画停止の有無	計画停止有り(運用スケジュールの変更可)	計画停止有り(運用スケジュールの変更不可)	計画停止無し		○ 【重複項目】 A.1.1.3. 計画停止の有無は、システムの可用性の実現レベルを表す項目でもあるため、重複項目となっている。 【運用コストへの影響】 計画停止有りの場合、事前のバックアップや、システム構成に応じた手順準備など、運用時のコストがかさむ。	0	計画停止有り(運用スケジュールの変更可)	事前の合意があれば、停止は可能。 [+] 運用時間外での停止だけで対応可能な場合	1	計画停止有り(運用スケジュールの変更不可)	24時間無停止での運用は必要ない。停止可能な時間が存在し、計画的な停止は可能。 [-] 運用スケジュールとしては停止可能な時間帯は存在しないが、事前の調整で停止が可能な場合 [+] 24時間無停止が要求される場合	2	計画停止無し	システムを停止できる時間帯が存在しない。 [-] 運用スケジュールとして停止可能な時間帯が存在し、計画停止の必要性がある場合		
C.2.2.1			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。		保守作業自動化の範囲	保守作業は全て手動で実施する	一部の保守作業を自動で実行する	全ての保守作業を自動で実行する			○ 【メトリクス】 保守作業とは、保守運用に伴うシステム基盤を維持管理するための作業を指し、点検作業やパッチ適用等のアップデート作業、領域拡張、デフラグ、ログローテート等を想定している。障害対応や復旧作業などは含まない。 【運用コストへの影響】 システム基盤の保守運用作業を自動化するためには、特別な運用管理ツールを導入したり、さまざまな作り込みを実施する必要がある。そのため導入コストは増大するが、ユーザが実施すべき保守運用作業が簡略化あるいはなくなると考えられるので、運用コストは減少する。	0	保守作業は全て手動で実施する	全ての保守作業を管理者が手動で実行することを想定。 [+] いくつかの保守作業を自動化する場合	1	一部の保守作業を自動で実行する	業務機能の起動・停止など定期的に行う処理は自動化するが、ログの削除など非定期に実行する処理は管理者が手動で実施することを想定。 [-] 全ての保守作業を手動で実行する場合 [+] 全ての保守作業を自動化する場合	2	全ての保守作業を自動で実行する	業務機能の起動・停止やスケジュールリングされたメンテナンス操作を全て自動で実行することを想定 [-] いくつかの機能は管理者が手動で実行することを想定する場合	
C.4.1.1			運用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。		開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する			【メトリクス】 開発用環境とは、本番環境とは別に開発専用を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。 【レベル】 開発フェーズでは開発環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの開発環境を設置しないを選択する。	0	システムの開発環境を設置しない	本番環境上で開発を行い、そのまま本番運用に使用する。 [+] 運用中も開発を実施するために、開発環境を用意する場合	1	運用環境の一部に限定した開発環境を設置する	非クラスタの開発環境を用意する。 [-] 開発環境を用意しない場合 [+] 本番環境と同等の開発環境を用意する場合	2	運用環境と同一の開発環境を設置する	本番環境と同等の開発用環境を設置することを想定。 [-] 本番環境では複数台存在するAPサーバを1台のみで開発環境を用意する場合	
C.4.2.1			試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目。		試験用環境の設置有無	システムの試験環境を設置しない	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			【メトリクス】 試験用環境とは、本番環境とは別に試験専用を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。 【レベル】 試験フェーズでは試験環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの試験環境を設置しないを選択する。	0	システムの試験環境を設置しない	試験用環境を用意しない。 [+] 試験用環境を用意する場合	1	システムの開発用環境と併用する	開発環境上で試験も実施する。 [-] 試験用環境を用意しない場合 [+] 開発環境とは別に試験用の環境を用意する場合	2	専用の試験用環境を設置する	開発環境とは別に試験用の環境も用意する。 [-] 開発環境と試験環境を併用する場合	
C.4.3.1			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。		マニュアル準備レベル	各製品標準のマニュアルを利用する	システムの通常運用のマニュアルを提供する	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、システム基盤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、システム基盤に対する保守作業(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。 【運用コストへの影響】 ユーザの運用に合わせたカスタマイズされたマニュアルは、作成するためにコストがかかるため導入コストが増大するが、ユーザが運用時に手順を調査する負担が減少するため運用コストは減少する。	0	各製品標準のマニュアルを利用する	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。 [+] ベンダよりマニュアルの提供を受け必要がある場合	2	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。 [-] 保守作業は全てベンダに依頼するため、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を作成する場合 [+] 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	3	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	ユーザの自営センターの運用ルールにのっとったマニュアルの作成を要望。 [-] ベンダの用意する一般的な運用マニュアルで良いような場合		

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	メトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム		
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件
C.4.4.1			リモートオペレーション	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。		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				○	【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。 【運用コストへの影響】 リモート監視を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、運用状況の確認のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。	0	リモート監視を行わない [+] 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	1	構内LANを介してリモート監視を行う [-] 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 [+] 各支店に配置されているクライアント機器類についてもリモートで集中監視を行う場合	2	遠隔地でリモート監視を行う [-] リモートで監視を行うのはセンターに配置されているサーバ機器類のみとし、各支店に配置されているクライアント機器類はコンソールにて直接監視してもらうような場合
C.4.4.2				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					○	【メトリクス】 リモート監視地点から実施できる操作の範囲を検討する。 【レベル】 定型処理のみリモート操作を実現するためのソフトウェアは安価であったり、任意のリモート操作を認める場合はセキュリティやその他の面での検討項目が増えることを考慮し、定型処理よりも任意のリモート操作を行う方のレベルを高く設定している。 【運用コストへの影響】 リモート操作を実装するためには、特別なハードウェア・ソフトウェアを導入する必要があり導入コストが増大する。しかし、メンテナンス操作のために管理者がわざわざサーバの設置場所まで移動する必要がなくなるため、運用コストは減少する。	0	リモート操作を行わない [+] リモートの管理端末を用意し、そこからメンテナンス操作を実行することを想定する場合	1	定型処理のみリモート操作を行う [-] リモートからの操作は実行しない場合 [+] 任意の操作を実行できるようにする場合	2	任意のリモート操作を行う [-] 特定の操作のみの実行ができればよいような場合	
C.4.5.1			外部システム接続	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。	外部システムとの接続有無	外部システムと接続しない	社内の外部システムと接続する	社外の外部システムと接続する					○	【メトリクス】 接続する場合には、そのインターフェースについて確認すること。	0	外部システムと接続しない [+] 履歴データを蓄積・分析を行うようなシステムに対してデータを送信するなど、連携する他システムが存在する場合	1	社内の外部システムと接続する [-] データのやり取りを行う多システムが存在しない場合 [+] 社外のシステムに接続して、データのやり取りを行う場合	2	社外の外部システムと接続する [-] システムと連携する外部のシステムが存在しない場合
C.5.1.1		サポート体制	保守契約(ハードウェア)	保守が必要な対象ハードウェアの範囲。		保守契約(ハードウェア)の範囲	保守契約を行わない	ベンダの自社製品(ハードウェア)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(システムを構成する全製品を対象)	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)			○	【レベル】 ベンダの自社製品(ハードウェア)に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。	1	ベンダの自社製品(ハードウェア)に対してのみ保守契約を行う [+] Slerを立てて、システム全体を調達するような場合	2	マルチベンダのサポート契約を行う(一部対象外を許容) [-] 複数製品についてのワンストップのサポート窓口を必要としない場合 [+] サポート対象外を許容せず、システムを構成する全ての製品についてワンストップのサポート窓口を必要とする場合	3	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) [-] 特殊な製品や、既存の機器を用いたシステムの構築を行う場合など、一部の製品に関して問い合わせ窓口を一本化する必要がない場合
C.5.2.1			保守契約(ソフトウェア)	保守が必要な対象ソフトウェアの範囲。	保守契約(ソフトウェア)の範囲	保守契約を行わない	ベンダの自社製品(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(システムを構成する全製品を対象)	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)			○	【レベル】 ベンダの自社製品(ソフトウェア)に対してのみサポート契約とは、システムを構成する製品個別の提供ベンダと、当該製品に対するサポート契約を行うことを意味しており、当該製品に対してのみサポートサービスが提供される契約形態のことである。 マルチベンダのサポート契約とは、システム全体に対するサポートサービスを提供するベンダと契約を行うことを意味しており、複数のベンダの製品から構成されるシステムに対してワンストップのサポート窓口が提供される契約形態のことである。 【運用コストへの影響】 サポート契約を行うと運用コストが増大するように感じられるが、問題が発生した際に必要となる費用が膨大となるため、サポート契約を行ったほうが結果として運用コストは小さくなる場合がある。	1	ベンダの自社製品(ソフトウェア)に対してのみ保守契約を行う [+] Slerを立てて、システム全体を調達するような場合	2	マルチベンダのサポート契約を行う(一部対象外を許容) [-] 複数製品についてのワンストップのサポート窓口を必要としない場合 [+] サポート対象外を許容せず、システムを構成する全ての製品についてワンストップのサポート窓口を必要とする場合	2	マルチベンダのサポート契約を行う(一部対象外を許容) [-] 特殊な製品や、既存の機器を用いたシステムの構築を行う場合など、一部の製品に関して問い合わせ窓口を一本化する必要がない場合	
C.5.3.1			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。	ライフサイクル期間	3年	5年	7年	10年以上					○	【メトリクス】 ここでのライフサイクルとは、次回のシステム更改までの期間と規定している。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。	0	3年 [+] 社内規定などにより、システムのライフサイクル期間が7年程度と定められているような場合	2	7年 [-] 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 [+] 内部統制等によりシステムで実行する業務を10年以上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	3
C.6.1.1	その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目。		内部統制対応の実施有無	内部統制対応にない	既存の社内規定に従って、内部統制対応を実施する	新規に規定を制定し、内部統制対応を実施する					○	【メトリクス】 ここでは内部統制対応の実施有無について確認する。内部統制対応の具体的な対応方法(オペレーションで実施するか、システムへの機能実装で実現するか等)については、有無の確認後に具体化して確認する。	0	内部統制対応にない [+] 対象システムではないが、部門の判断により内部統制対応を実施する場合	1	既存の社内規定に従って、内部統制対応を実施する [-] 内部統制実施の対象システムではないため、対応を実施しない場合 [+] 既存の規定は存在しないが、本システムを構築するに際して、新たな規定を策定するような場合	1	既存の社内規定に従って、内部統制対応を実施する [-] 順守すべき法令や社内の内部統制規定等が存在しない場合 [+] 既存の規定は存在しないが、本システムを構築するに際して、新たな規定を策定するような場合
C.6.2.1		サービスデスク	ユーザの問合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。	サービスデスクの設置有無	サービスデスクの設置にない	既存のサービスデスクを利用する	新規にサービスデスクを設置する						○	【メトリクス】 ここでは、ユーザとベンダ間におけるサービスデスクの設置の有無について確認する。サービスデスク機能の具体的な実現方法については、有無の確認後に具体化して確認する。	0	サービスデスクの設置にない [+] サービスデスクを設置する場合	1	既存のサービスデスクを利用する [-] サービスデスクを設置しない場合 [+] 初めて取引を行うベンダで、既存のサービスデスクが存在しないような場合	2	新規にサービスデスクを設置する [-] 既存のサービスデスク機能を利用するような場合

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム					
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件			
D.1.1.1	移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無。(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。)		システム移行期間	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			1	3ヶ月未満 [+] 中長期間で進める場合	システムを短期間で構築する必要がある。 [+] さらに長期期間が必要な場合	4	2年未満 [+] 期間短縮の場合	年度を跨いで移行を進める必要がある。 [+] さらに長期期間が必要な場合	5	2年以上 [+] 期間短縮の場合	移行の計画から稼働まで安全性を最優先にして進める必要がある。 [+] 期間短縮の場合
D.1.1.2						システム停止可能日時	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		【マトリクス】 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ることを示す。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。	1	5日以上 [+] さらに停止を多くする場合 [+] 停止を少なくする場合	業務への影響が少なく数日以上はシステム停止可能。 [+] 停止を増やす場合	4	利用の少ない時間帯(夜間など) [+] 停止を増やす場合	業務が比較的に少ない時間帯にシステム停止が可能。 [+] 停止を増やす場合	5	移行のためのシステム停止不可 [+] 停止時間を確保する場合	システム停止時間は最短にする必要がある。 [+] 停止時間を確保する場合
D.1.1.3						並行稼働の有無	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。関係項目にF.4.2.3、F.4.4.3がある。	0	無し [+] 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	移行のためのシステム停止期間が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可能であり、並行稼働しない場合	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	1	有り	移行のためのシステム停止不可のため、移行時のリスク軽減を最優先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
D.2.1.1	移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するか程度。		拠点展開ステップ数	単一拠点のため規定無し	一斉展開	5段階未満	10段階未満	20段階未満	20段階以上		【レベル】 拠点展開時のリスクによっては難易度が逆転し、一斉展開の難易度が高くなる場合もある。対象システムについて、拠点毎に展開時のリスクを考慮して拠点展開ステップ数を判断すること。	0	単一拠点のため規定無し [+] 展開を検討する必要がある場合	システムが単一で展開を規定する必要がない。 [+] 展開を検討する必要がある場合	1	一斉展開	効率を優先させて一斉に切り替える。段階的に移行させる必要性は低い。 [+] 段階的に展開が必要な場合	2	5段階未満 [+] 一斉展開する場合 [+] 段階数を増やす必要がある場合	段階的展開が必要である。 [+] 段階数を増やす必要がある場合	
D.2.1.2					業務展開ステップ数	単一業務のため規定無し	全業務一斉切り替え	4段階未満	6段階未満	10段階未満	10段階以上		【レベル】 業務展開時のリスクによっては難易度が逆転し、全業務一斉切り替えの難易度が高くなる場合もある。対象システムについて、業務毎に展開時のリスクを考慮して業務展開ステップ数を判断すること。	0	単一業務のため規定無し [+] 展開を検討する必要がある場合	システムが単一で展開を規定する必要がない。 [+] 展開を検討する必要がある場合	1	全業務一斉切り替え	効率を優先させて一斉に切り替える。段階的に移行させる必要性は低い。 [+] 段階的に展開が必要な場合	2	4段階未満 [+] 一斉展開する場合 [+] 段階数を増やす必要がある場合	段階的展開が必要である。 [+] 段階数を増やす必要がある場合	
D.3.1.1	移行対象	(機器)	移行設備	移行前の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。	設備・機器の移行内容	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。	0	移行対象無し [+] 既存設備機器が存在する場合	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	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の更改程度が大きい場合	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	業務アプリケーションを更改はせずに、老朽化または性能向上等の対策を必要がある。 [+] ハードウェアのみ入れ替える場合 [+] 業務アプリケーションの更改が有る場合		
D.4.1.1			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)。	移行データ量	移行対象無し	1TB未満	1PB未満	1PB以上				1	1TB未満 [+] 1TB以上の場合	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	2	1PB未満	1PB(ペタバイト)未満のデータを移行する必要がある。 [+] 1PB以上の場合	3	1PB以上	1PB(ペタバイト)以上のデータを移行する必要がある。 [+] 1PB未満の場合		
D.4.1.2				移行データ形式		移行対象無し	移行先と形式が同一	移行先と形式が異なる				【マトリクス】 データ形式は、アプリケーションに依存したフォーマット、テーブル形式や文字コードなど、新システムに移行するために考慮すべきデータ形式のパターンを指す。 【レベル】 移行データ形式のパターンが複数ある場合には、それぞれについてデータ形式を確認すること。	1	移行先と形式が同一 [+] データ形式の変更が必要な場合	データ形式を現状のままで使用する。 [+] データ形式の変更が必要な場合	2	移行先と形式が異なる	業務の効率化や統合化等によって、データ形式の変更が必要である。 [+] 移行データの形式を変更しない場合	1	移行先と形式が同一	データの継続性や他システムとの親和性を担保するため、データ形式を現状のままで使用する。 [+] データ形式の変更が必要な場合		
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき情報セキュリティに関する組織規程やルール、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) ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール	順守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り					【マトリクス】 規程、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。 例) ・国内/海外の法律 不正アクセス禁止法・不正競争防止法・プロバイダ責任法・改正個人情報保護法・SOX法・ EU一般データ保護規則(GDPR)・特定電子メール送信適正化法・電子署名法 など ・資格認証 プライバシーマーク・ISMS/ITSMS/BCMS/CSMS・ISO/IEC27000系・PCI DSS・ クラウド情報セキュリティ監査・TRUSTe など ・ガイドライン FISC・FISMA/NIST800・政府機関の情報セキュリティ対策のための統一基準 など ・その他ルール 情報セキュリティポリシー など 【レベル1】 構築するシステムが関係する国や地域によって、順守すべき法令やガイドラインが異なることに注意すること。	0	無し [+] 順守すべき規程、法令、ガイドライン等が存在する場合	ユーザ要件に応じてレベルを判断する必要がある。 [+] 順守すべき規程、法令、ガイドライン等が存在する場合	0	無し	ユーザ要件に応じてレベルを判断する必要がある。 [+] 順守すべき規程、法令、ガイドライン等が存在する場合					

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム				
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件		
E.2.1.1		セキュリティリスク分析	セキュリティリスク分析	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。		リスク分析範囲	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				【マトリクス】 システム開発中に実施するセキュリティリスク分析では、ソフトウェアのサポート終了や暗号の危殆化等の運用期間に顕在化するリスクも考慮する。 【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。	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。	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	2	開発範囲	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。また、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、システム全体のリスクを分析する必要がある。 [-] データの移動や更新等が生じず、それらに伴った情報へのアクセス権限の変化等による脅威が存在しない(あるいは許容する)場合
E.3.1.1			セキュリティ診断	対象システムや、各種ドキュメント(設計書や環境定義書、実装済みソフトウェアのソースコードなど)に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。		ネットワーク診断実施の有無	無し	有り					【マトリクス】 ネットワーク診断には、目視による設定の確認や、疑似攻撃を実施することにより脆弱性を発見する診断(ペネトレーションテスト)、ネットワーク上のサーバや通信機能をもつソフトウェアなどに対する脆弱性調査等がある。 【レベル1】 ネットワーク診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。	1	有り	ネットワークを介し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、ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、ネットワークを介した攻撃への対策が十分に検討し、各種ドキュメントが作成される場合。	1	有り	重要情報を取り扱うため、内部ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、内部ネットワーク経由での攻撃への対策が十分に検討し、各種ドキュメントが作成される場合。	1	有り	ネットワークを介した、外部からの不特定多数の攻撃者からの脅威にさらされる。また、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、ネットワーク経由での攻撃に対する脆弱性を分析する必要がある。 [-] セキュリティに関する専門的な知識を有する者により、ネットワークを介した攻撃への対策が十分に検討し、各種ドキュメントが作成される場合。
E.3.1.2				Web診断実施の有無	無し	有り							【マトリクス】 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を言う。 【レベル1】 Web診断は、システム運用開始前に実施するだけでなく、システム運用中の定期的な実施も検討する。	1	有り	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	1	有り	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	1	有り	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
E.5.1.1		アクセス・利用制限	認証機能	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カード等を用いた認証等がある。		管理権限を持つ主体の認証	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			【マトリクス】 管理権限を持つ主体とは、システムの管理者や業務上の管理者を指す。	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	2	複数回の認証	攻撃者が管理権限を手に入れることによる、情報漏洩等の脅威に対抗するため、複数回の認証を実行する必要がある。	2	複数回の認証	攻撃者が管理権限を手に入れることによる、情報漏洩等の脅威に対抗するため、複数回の認証を実行する必要がある。 [-] 外部ネットワーク越しに管理権限を持つ主体がアクセスできない等の場合
E.5.2.1			利用制限	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、ソフトウェアやハードウェアにより制限するかを確認するための項目。 例) ドアや保管庫の施錠、USBやCD-RWやキーボードなどの入出力デバイスの制限、コマンド実行制限など。		システム上の対策における操作制限度	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					【マトリクス】 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いうため、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	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いうため、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	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いうため、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

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル						運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム	
							0	1	2	3	4	5			選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件
E.6.1.1		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。		伝送データの暗号化の有無	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、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。	1	認証情報のみ暗号化 [-] 認証情報をネットワークを経由して送信しない場合	2	重要情報を暗号化 ローカルネットワーク経由で重要情報を送付する場合においても、特に重要な情報については、盗聴等の脅威に対抗するために、伝送データを暗号化する必要がある。 (伝送データを暗号化することにより、性能が低下する可能性がある) [-] 専用線を用いる等の物理的な対策が実施されている場合/ローカルネットワーク上での盗聴の脅威については許容する場合/機密性は求められないが完全性が求められる重要情報を扱う場合	2	重要情報を暗号化 ローカルネットワーク経由で重要情報を送付する場合においても、特に重要な情報については、盗聴等の脅威に対抗するために、伝送データを暗号化する必要がある。 (伝送データを暗号化することにより、性能が低下する可能性がある) [-] 専用線を用いる等の物理的な対策が実施されている場合/ローカルネットワーク上での盗聴の脅威については許容する場合/機密性は求められないが完全性が求められる重要情報を扱う場合
E.6.1.2						蓄積データの暗号化の有無	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、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。	1	認証情報のみ暗号化 [-] 認証を実施しない場合	2	重要情報を暗号化 データベースやバックアップテープ等に格納されている個人情報等やパスワード等の重要情報の漏洩の脅威に対抗するために、蓄積データを暗号化する必要がある。 (蓄積データを暗号化することにより、性能に影響する可能性がある) [-] 耐タンパデバイスの利用、認証対策、運用対策等の他の複数の対策により、安全性が確保されている場合/機密性は求められないが完全性が求められる重要情報を扱う場合	2	重要情報を暗号化 データベースやバックアップテープ等に格納されている個人情報等やパスワード等の重要情報の漏洩の脅威に対抗するために、蓄積データを暗号化する必要がある。 (蓄積データを暗号化することにより、性能に影響する可能性がある) [-] 耐タンパデバイスの利用、認証対策、運用対策等の他の複数の対策により、安全性が確保されている場合/機密性は求められないが完全性が求められる重要情報を扱う場合
E.7.1.1		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 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。		ログの取得	実施しない	実施する						【マトリクス】 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。 取得したログは個々のログを確認するだけでなく、複数のログを組み合わせて相関分析することも検討する。必要に応じて、ログと作業記録との突き合わせも行う。 ・ログイン/ログアウト履歴(成功/失敗) ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ等	1	実施する 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」「その結果、どのようになったか」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)	1	実施する 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」「その結果、どのようになったか」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)	1	実施する 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」「その結果、どのようになったか」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)
E.7.1.2						ログ保管期間	6ヶ月	1年	3年	5年	10年以上 有期	永久保管			0	6ヶ月 不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [-] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合	2	3年 不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [-] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合	3	5年 不正行為を確認する、また、正しく処理された証跡を保持するために、適切な期間、ログを保管する必要がある。 [-] ログの確認間隔が短い場合 [+] バックアップ等の容量が確保できる場合
E.7.1.3						不正監視対象(装置)	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					【マトリクス】 不正監視対象(装置)とは、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マトリクス。	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。	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。	2	システム全体 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。外部ネットワーク経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する必要がある。
E.7.1.4						不正監視対象(ネットワーク)	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					【マトリクス】 不正監視対象(ネットワーク)とは、ネットワーク上の不正なパケット等を監視するためのログの取得範囲を確認するマトリクス。	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、監視対象とするネットワークの範囲を定めておく必要がある。	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、監視対象とするネットワークの範囲を定めておく必要がある。	2	システム全体 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、監視対象とするネットワークの範囲を定めておく必要がある。外部ネットワーク経由での攻撃等により攻撃範囲が限定されないことを想定し、システム全体に対して監視を実施する必要がある。
E.7.1.5						不正監視対象(侵入者・不正操作等)	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					【マトリクス】 不正監視対象(侵入者・不正操作等)とは、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を意味する。	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、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。 [-]入退室管理、操作制限等の対策が十分に施されている場合	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、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。	2	システム全体 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、監視対象とするフロア、エリア等の物理的な範囲を定めておく必要がある。

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル					運用 コスト への 影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム			
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件	
E.8.1.1	ネットワーク 対策	ネットワーク制 御	不正な通信を遮断するための制御を実施 するかを確認するための項目。	通信制御	無し	有り						【レベル1】 通信制御を実現するには、ファイアウォール、IPS、URLフィルタ、メールフィルタ等の導 入を検討する必要がある。	1	有り	踏み台攻撃等の脅威や、情報の持ち 出しを抑止するために、不正な通信を 遮断等のネットワーク制御を実施する 必要がある。 [-] 踏み台等の脅威を許容する場合	1	有り	踏み台攻撃等の脅威や、情報の持ち 出しを抑止するために、不正な通信を 遮断等のネットワーク制御を実施する 必要がある。 [-] 踏み台等の脅威を許容する場合	1	有り	踏み台攻撃等の脅威や、情報の持ち 出しを抑止するために、不正な通信を 遮断等のネットワーク制御を実施する 必要がある。 [-] 踏み台等の脅威を許容する場合
E.8.2.1		不正検知	ネットワーク上において、不正追跡・監視 を実施し、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。	不正通信の 検知範囲	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				【マトリクス】 検知範囲の設定に応じて、IDS等の導入を検討する必要がある。	1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	不正な通信を確認し、対策を迅速に実 施すうために、不正検知を実施する必 要がある。	1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	不正な通信を確認し、対策を迅速に実 施すうために、不正検知を実施する必 要がある。	1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	不正な通信を確認し、対策を迅速に実 施すうために、不正検知を実施する必 要がある。	
E.8.3.1		サービス停止 攻撃の回避	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。	ネットワー クの輻輳対策	無し	有り						1	有り	DoS/DDoS攻撃のサービス停止攻撃に 対応する必要がある。 (可用性と関連する) [-] DoS/DDoS攻撃については、可用 性対策にてある程度の対策を実施し、 それ以上は許容する場合	1	有り	DoS/DDoS攻撃のサービス停止攻撃に 対応する必要がある。 (可用性と関連する) [-] DoS/DDoS攻撃については、可用 性対策にてある程度の対策を実施し、 それ以上は許容する場合	1	有り	DoS/DDoS攻撃のサービス停止攻撃に 対応する必要がある。 (可用性と関連する) [-] DoS/DDoS攻撃については、可用 性対策にてある程度の対策を実施し、 それ以上は許容する場合	
E.9.1.1	マル ウ ェ ア 対 策	マルウェア対策	マルウェア(ウイルス、ワーム、ボット等) の感染を防止する、マルウェア対策の実 施範囲やチェックタイミングを確認するた めの項目。 対策を実施する場合には、ウイルス定義 ファイルの更新方法やタイミングについ ても検討し、常に最新の状態となるよう にする必要がある。	マルウェア対 策実施範囲	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					1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	マルウェアの感染により、サービス停 止等の脅威に対抗するために、マル ウェア対策を実施する必要がある。 [-] 攻撃対象となりにくいOS等を利用 する場合	1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	マルウェアの感染により、重要情報が 漏洩する脅威等に対抗するために、マ ルウェア対策を実施する必要がある。 [-] 攻撃対象となりにくいOS等を利用 する場合	1	重要度が 高い資産 を扱う範 囲、ある いは、外 接部分	マルウェアの感染により、重要情報が 漏洩する脅威等に対抗するために、マ ルウェア対策を実施する必要がある。 [-] 攻撃対象となりにくいOS等を利用 する場合	
E.10.1.1		W e b 対 策	Web実装対策	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。	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	無し	対策の強 化					【マトリクス】 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。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。	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	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	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
E.10.1.2						WAFの導入 の有無	無し	有り					【マトリクス】 WAFとは、Web Application Firewallのことである。	0	無し	重要情報を取り扱わないため、WAFを 導入しての対策は実施しない。 [+] 内部ネットワークを経由した攻撃に よる脅威を想定する場合	0	無し	外部ネットワークへの接続については 想定しない。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。 [+] Webサーバへの対策、不正アクセス 防止、ログの定期的な確認等が実施さ れている場合	1	有り
F.1.1.1	シ ス テ ム 環 境 ・ エ コ ロ ジ	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社内基準や法令、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	構築時の制 約条件	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (全ての制 約を適用)				【マトリクス】 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環境を整備する必要がある。ま た運用予定地での構築が出来ず、別地にステージング環境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。	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	1	制約有り (重要な 制約のみ 適用)	社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 [+] 法や条例の順守よりも高度な社内 基準の制約を受け、かつ、全てに対応 することが必要な場合	1	制約有り (重要な 制約のみ 適用)	法の制約などを受ける場合を想定。 [-] 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 [+] 法や条例の順守よりも高度な社内 基準の制約を受け、かつ、全てに対応 することが必要な場合
F.1.2.1			運 用 時 の 制 約 条 件	運用時の制約 条件	運用時の制約となる社内基準や法令、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 ・リモートからの運用の可否 など	運用時の制 約条件	制約無し	制約有り (重要な制 約のみ適 用)	制約有り (全ての制 約を適用)					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	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	1	制約有り (重要な 制約のみ 適用)

非機能要求グレード 2018 システム基盤の非機能要求に関するグレード表

グレード表

項番	大項目	中項目	小項目	小項目説明	重複項目	マトリクス (指標)	レベル					運用コストへの影響	備考	社会的影響が殆ど無いシステム		社会的影響が限定されるシステム		社会的影響が極めて大きいシステム				
							0	1	2	3	4			5	選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件		
F.2.1.1		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数。	○	ユーザ数	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				【重複項目】 B.1.1.1。ユーザ数は性能・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ため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。	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	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	2	不特定多数のユーザが利用	国民全体がアクセスする可能性があるような場合を想定。 [-] 一定の上限値を設定することが可能な場合
F.2.2.1			クライアント数	システムで使用され、管理しなければならないクライアントの数。		クライアント数	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				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	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。 [+] 上限台数を設定できない場合	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。 [+] 上限台数を設定できない場合	
F.2.3.1			拠点数	システムが稼働する拠点の数。		拠点数	単一拠点	複数拠点				【レベル1】 拠点数を合意した場合は具体的な値を設定すること。	0	単一拠点	単一拠点を想定。 [+] 複数拠点の場合	1	複数拠点	複数拠点を想定。 [-] 単一拠点の場合	1	複数拠点	複数拠点を想定。 [-] 単一拠点の場合	
F.2.4.1			地域的広がり	システムが稼働する地域的な広がり。		地域的広がり	拠点内	同一都市内	同一都道府県内	同一地方	国内	海外	【レベル】 レベル5になると、多言語対応などの考慮も必要となる。 また、国内であっても範囲が広がるにつれて、ネットワークや物流、サポートなどの面での対応が必要となる。	0	拠点内	アクセス範囲を拠点内とし、外部からのアクセスがない場合を想定。 [+] リモートアクセスを許すなどアクセス範囲が拠点外にも広がる場合	0	拠点内	アクセス範囲を拠点内とし、外部からのアクセスがない場合を想定。 [+] 他の事業所から利用させる場合	4	国内	アクセス範囲は国内とすることを想定。 [-] ユーザ権限を企業や団体内ユーザに限定する場合 [+] インターネットシステムなどで、アクセス範囲が国外にも広がる場合
F.2.5.1			特定製品指定	ユーザの指定によるオープンソース製品や第三者製品(ISV/IHV)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。		特定製品の採用有無	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				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	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	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	
F.3.1.1		適合規格	製品安全規格	提供する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。	規格取得の有無	規格取得の必要無し	UL60950相当取得					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	1	UL60950相当取得	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	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		
F.3.2.1			環境保護	提供する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。	規格取得の有無	規格取得の必要無し	RoHS指令相当取得				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	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	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			
F.4.1.1	機材設置環境条件	耐震/免震	地震発生時にシステム設置環境で耐える必要のある実効的な最大震度を規定。建屋が揺れを減衰するなどの工夫により、外部は震度7超でも設置環境では実効的に最大震度4程度になる場合には震度4よりレベルを設定する。なお、想定以上の揺れではサービスを継続しないでも良い場合には、その想定震度でレベルを設定する。	耐震震度	対策不要	震度4相当(50ガル)	震度5弱相当(100ガル)	震度6弱相当(250ガル)	震度6強相当(500ガル)	震度7相当(1000ガル)	【マトリクス】 設置環境での実効的な震度は、屋外の振動がそのまま伝わる建屋の場合は外部の震度と設置環境の震度はほぼ一致すると考えられるので、外部震度からレベルを設定すればよい。ただし、建屋の免震設備などにより、設置環境での最大震度を低く保証できる場合にはその震度を実効的な震度としてレベル設定が可能と考えられる(ユーザからの特段の要請を受けて、より高いレベルで設定する場合もあり)。なお、一定の震度以上では周辺のシステム利用者がシステムを利用できる環境に無いなどで、サービスの継続が不要となる場合は、その震度からレベル設定することも考えられる。いずれに於いても建屋の耐震震度を超える水準での設定には無理がある。 【レベル0】 地震発生によるサービス停止などのリスクを受け入れる心積もりが別途必要となる。	2	震度5弱相当(100ガル)	震度5弱相当を想定。 [-] 免震構造の建屋に設置するなど建屋と設置環境とを見合わせレベル変更する場合 [+] 特に値が指定された場合は相応するレベルに変更。免震構造を持たないオフィス内などに設置するなどラック転倒などによる人災を避けるために耐震ラックの利用などレベルを上げることも配慮が必要な場合	3	震度6弱相当(250ガル)	震度6弱相当を想定。 [-] 免震構造の建屋に設置するなど建屋と設置環境とを見合わせレベル変更する場合 [+] 特に値が指定されるなど建屋と設置環境とを見合わせ相応するレベルに変更する場合	4	震度6強相当(500ガル)	震度6強相当を想定。 [-] 免震構造の建屋に設置するなど建屋環境と機器環境を総合して考慮する場合 [+] 特に震度7など強い地震に相応する値が指定された場合		
F.4.2.1		スペース	どの程度の床面積(WxD)/高さが必要かの項目。保守作業用スペースについても考慮する。また、移行時には新旧システムが並行稼働可能なスペースの確保が可能か否かについても確認が必要である。可能であれば事前確認を実施する。	設置スペース制限(マシンルーム)	スペースに関する制限無し	フロア設置用機材を用いて構成	ラックマウント用機材を用いて構成			【マトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。	2	ラックマウント用機材を用いて構成	ラックマウントなどでの搭載を想定。 [-] 設置に関して制限がない場合	2	ラックマウント用機材を用いて構成	ラックマウントなどでの搭載を想定。 [-] 設置に関して制限がない場合	2	ラックマウント用機材を用いて構成	センターでのラックマウントを想定。 [-] 設置に関して制限がない場合			
F.4.2.2					設置スペース制限(事務所設置)	スペースに関する制限無し	専用のスペースを割当て可能	人と混在するスペースに設置必要		【マトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル】 設置スペース制限は前提条件として既に規定されていると捉え、その要求に対してシステムを設置する場合の難易度をレベルとしている。スペース確保の視点での難易度ではないことに注意。	1	専用のスペースを割当て可能	オフィスフロア内のサーバ・コーナーなどに設置することを想定。 [-] 人がほとんど立ち入らない場所への設置の場合 [+] 操作や監視などの関係上、仕切りなど無しに人と混在するスペースに設置が必要な場合	2	人と混在するスペースに設置必要	端末機などフロントエンド業務用の機材を想定。 [-] 業務的に人との混在が不要な場合	2	人と混在するスペースに設置必要	端末機などフロントエンド業務用の機材を想定。 [-] 業務的に人との混在が不要な場合			