参考資料01 非機能要件 IPA 10 活用シート

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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。 【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動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動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）	[本番環境] 土曜日、日曜日を除く。（月曜日～金曜日は祝日であっても稼働する。） 9時～18時は事業者と本機関が利用 18時～20時は、本機関のみ利用可能 以降はバッチ稼働時間の設計による。 なお、月複数回の時間延長を想定 [検証環境] 平日のみの稼働とし運用時間は本番環境と同様 [研修環境] 平日のみの稼働とし運用時間は本番環境と同様	4.15.1. 基本事項
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。 【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。				
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）	計画停止は可能であるが、事前に通知を行ったうえで、本機関の合意を得ること。	4.15.1. 基本事項
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		【メトリクス】 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。	5	全ての業務		4.5.1. 可用性要件
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	○	【メトリクス】 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	サーバ等の切替時間は2時間以内を想定	ー
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					【メトリクス】 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		4.9.1.継続性に関する基本要件
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）				【メトリクス】 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。	2	1営業日前の時点（日次バックアップからの復旧）		4.9.2.継続性に関する目標値
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			【メトリクス】 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。	2	12時間以内		4.9.2.継続性に関する目標値

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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					【メトリクス】 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。	2	全ての業務		4.9.2.継続性に関する目標値
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		【メトリクス】 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。	3	一週間以内に再開	社会インフラが正常となっている状況下で一週間以内に再開	ー
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%		4.5.1. 可用性要件
A.2.1.1		耐障害性	サーバ	サーバで発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定のサーバで冗長化	全てのサーバで冗長化					【メトリクス】 冗長化における機器、コンポーネントは、冗長化の単位を表し、機器は筐体を複数用意することによる冗長化、コンポーネントは筐体を構成する部品（ディスク、電源、FAN、ネットワークカード等）を複数用意することによる冗長化を指す。 また、仮想化技術の適用により、同一ハードウェア上にサーバ機能を集約させることで、冗長化に必要なハードウェア所要量を削減することも可能である。いずれにしても、ハードウェア上で実現される業務継続性の要求を満たすよう機器の冗長化を検討する必要がある。 【レベル1】 特定のサーバで冗長化とは、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、それを実装するサーバを想定してレベルを設定する。				
A.2.1.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 サーバを構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのミラー化や、ネットワークIFカードの2重化など）。				
A.2.2.1			端末	端末で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	共用の予備端末を設置	業務や用途毎に予備端末を設置									
A.2.2.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 端末を構成するコンポーネントとして、内蔵ディスクや、電源、FANなどを必要に応じて冗長化することを想定している（例えば内蔵ディスクのRAID構成など）。				
A.2.3.1			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化					【レベル1】 特定の機器のみとは、ネットワークを構成するルータやスイッチの内、冗長化したサーバを収容するスイッチなどを想定している。				
A.2.3.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 ネットワーク機器を構成するコンポーネントとして、電源やCPU、FANなどを必要に応じて冗長化することを想定している。				
A.2.4.1			ネットワーク	ネットワークの信頼性を向上させるための要求。			回線の冗長化	冗長化しない	一部冗長化	全て冗長化する					【メトリクス】 回線の冗長化とは、ネットワークを構成する伝送路（例えばLANケーブルなど）を物理的に複数用意し、一方の伝送路で障害が発生しても他方での通信が可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。				
A.2.4.2							経路の冗長化	冗長化しない	一部冗長化	全て冗長化する					【メトリクス】 経路の冗長化とは、ネットワーク内でデータを送受信する対象間で、データの流れる順序（経由するルータの順序）を複数設定することで、ある区間で障害が発生しても、他の経路で迂回し通信を可能な状態にすること。 【レベル1】 一部冗長化とは、基幹のネットワークのみ冗長化するケースや、業務データの流れるセグメントなどを想定している。				
A.2.4.3							セグメント分割	分割しない	サブシステム単位で分割	用途に応じて分割					【レベル2】 用途とは、監視やバックアップなどの管理系の用途から、オンライン、バッチなどの業務別の用途を示している。 サブシステム単位で分割したなかで、更に用途に応じてセグメントを分割することを想定している。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
A.2.5.1			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化					【メトリクス】 NAS、iSCSI対応の装置を含む。 ただしNASやiSCSIはLANなどのネットワークに接続して利用するため、NASやiSCSIの接続環境の耐障害性対策は小項目A.2.4ネットワークに含まれる。 【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毎に異なる場合を想定している。				
A.2.5.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化					【レベル1】 ストレージを構成するコンポーネントとして、ディスクを除く、CPUや電源、FAN、インターフェースなどを必要に応じて冗長化することを想定している。				
A.2.5.3							冗長化（ディスク）	非冗長構成	単一冗長	多重冗長					【レベル1】 単一冗長とは、単一箇所の障害であれば、サービス継続可能な冗長構成のことである。 【レベル2】 多重冗長とは、同時に複数の箇所が障害の状態となっても、サービス継続可能な冗長構成のことである。				
A.2.6.1			データ	データの保護に対しての考え方。	○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ				【重複項目】 C.1.2.7。バックアップ方式は、バックアップ運用設計を行う上で考慮する必要があり、運用・保守性と重複項目としている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。				
A.2.6.2					○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧					【重複項目】 C.1.2.1。可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。				
A.2.6.3							データインテグリティ	エラー検出無し	エラー検出のみ	エラー検出＆再試行	データの完全性を保障（エラー検出＆訂正）				【メトリクス】 データに対して操作が正しく行えること、操作に対して期待した品質が得られること、またデータへの変更が検知可能であることなどを物理レベルで保証する。 【レベル】 仕組みの実装は、製品、業務アプリケーションによる検出を含む。				
A.3.1.1		災害対策	システム	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要求。			復旧方針	復旧しない	限定された構成でシステムを再構築	同一の構成でシステムを再構築	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			【メトリクス】 大規模災害のための代替の機器として、どこに何が必要かを決める項目。 【レベル】 レベル1および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。 レベル2および4の同一の構成とは、復旧後も復旧前と同じサービスレベルを維持するため、本番環境と同一のシステム構成を必要とすることを意味する。 レベル1および2のシステムを再構築を選択する場合、被災後の再構築までを契約の範囲として考えるのではなく、被災したサイトあるいは共用センターなどの設備を利用して、あくまでシステムを再構築する方針とすることを要求するものである。 一方レベル3および4のDRサイトで構築は、指定されたDRサイトに復旧用のシステムを構築するところまでを含む。	2	同一の構成でシステムを再構築	一週間以内に復旧できればDR環境は不要	ー
A.3.2.1			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などの要求。			保管場所分散度	外部保管しない	1ヵ所	1ヵ所（遠隔地）	2ヵ所（遠隔地）					2	1ヵ所（遠隔地）	ネットワークの異なるストレージ等にバックアップすること。	4.9.3.継続性に係る対策
A.3.2.2							保管方法	媒体による保管	同一サイト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						1	同一サイト内の別ストレージへのバックアップ	ネットワークの異なるストレージ等にバックアップすること。	4.9.3.継続性に係る対策
A.3.3.1			付帯設備	各種災害に対するシステムの付帯設備での要求。			災害対策範囲	対策を実施しない	特定の対策を実施する	想定する全ての対策を実施する					【メトリクス】 付帯設備については、システム環境・エコロジーにおいてF.4.1.1の耐震震度、F.4.4.4の停電対策で、災害対策の一部として要求を具体化している。 【レベル】 想定する災害対策としては、以下が考えられる。 ・地震対策 ・瞬電・停電対策 ・火災対策 ・漏電対策 ・雷対策 ・水害対策 ・電界・磁界対策				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
A.4.1.1		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧				【重複項目】 C.3.1.1。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリー機能充足率など）を定義するケースもあるが、可用性としては、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。				
A.4.1.2					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要					【重複項目】 C.3.1.2。復旧作業は、可用性と運用・保守性に共通して含まれている。運用・保守性では、復旧目標の運用への影響という観点でその作業を確認するが、可用性は、それを実現するための手段として確認する。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。	1	一部の業務について代替業務運用が必要	システム復旧後、当日分のデータについては再入力を想定	ー
A.4.2.1			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。	3	業務停止となる障害の全ての範囲		4.12.5.総合テスト要件
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。 それぞれのメトリクスに於いて、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。	1	上限が決まっている	02_主要業務量一覧「想定ユーザ及びログイン数」シートに記載	要件定義書別紙02_主要業務量一覧
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					【メトリクス】 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。	1	同時アクセスの上限が決まっている	200程度。全ユーザの1割を想定。	要件定義書別紙02_主要業務量一覧
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時保存分などがある。 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。	1	主要なデータ量のみが明確である		要件定義書別紙02_主要業務量一覧
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						【メトリクス】 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。	1	主な処理のリクエスト件数のみが明確である		要件定義書別紙02_主要業務量一覧
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						【メトリクス】 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、確定度合も含め、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。	1	主な処理の処理件数が決まっている		要件定義書別紙02_主要業務量一覧
B.1.1.6							業務機能数	業務機能が整理されている	確定した業務機能一覧が作成されている	業務機能一覧はあるが、確定していない					【メトリクス】 要件定義時には業務機能一覧はレベルの差があっても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、確定度合も含め、想定しておく。				
B.1.2.1			業務量増大度	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。	2	1.5倍	業務量増大度については、、運用報告書により分析、評価し見直す	ー

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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。	2	1.5倍		ー
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。	2	1.5倍		ー
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		【メトリクス】 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。	2	1.5倍		ー
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		【メトリクス】 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。	2	1.5倍		ー
B.1.2.6							業務機能数増大率	1倍	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 業務機能数増大率を評価する際は、機能の粒度（1機能あたりの見積規模、サービス範囲など）は具体的数値を示すことが望ましい。 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。				
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。	4	10年以上有期	10年とする。	4.15.4.1. ログ出力・蓄積・監視要件
B.1.3.2							対象範囲	オンラインで参照できる範囲	アーカイブまで含める						【メトリクス】 保管対象のデータを配置する場所を決める。保管場所によっては参照するための手間がかかる場合がある。また、バックアップの取得方法などへの配慮が必要になる。				
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。	3	90%		4.4.1. 応答時間
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。	3	90%		4.4.1. 応答時間
B.2.1.3							縮退時レスポンス順守率	縮退をしない	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。				
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。	1	所定の時間内に収まる	6時間以内に収めること。	4.4.1. 応答時間
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。	1	所定の時間内に収まる	6時間以内に収めること。	4.4.1. 応答時間

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
B.2.2.3							縮退時レスポンス順守度合い	縮退をしない	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。				
B.2.3.1			オンラインスループット	オンラインシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、単位時間にどれだけの量の作業ができるかを確認する。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・縮退運転時毎に処理余裕率を決める、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：データエントリ件数/時間、頁めくり回数/分、TPSなど）			通常時処理余裕率	1倍 （余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 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。				
B.2.3.2							ピーク時処理余裕率	1倍 （余裕無し）	1.2倍	1.5倍	2倍	3倍	10倍以上		【レベル】 ここでの余裕率は、システム全体で処理できるトランザクション量を示す。例えば、レベル3（2倍）であれば、2倍のトランザクションを処理できることを言う。 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。				
B.2.3.3							縮退時処理余裕率	縮退をしない	通常時の1/2の処理が出来る	通常時と同様に処理が出来る									
B.2.4.1			バッチスループット	バッチシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、どの程度のスループットを確保すべきか確認する。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・縮退運転時毎に処理余裕率を決める。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：人事異動情報一括更新処理、一括メール送信処理など）			通常時処理余裕率	1倍 （余裕無し）	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。				
B.2.4.2							ピーク時処理余裕率	1倍 （余裕無し）	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。				
B.2.4.3							縮退時処理余裕率	縮退をしない	通常時の1/2の処理が出来る	通常時と同様に処理が出来る									
B.2.5.1			帳票印刷能力	帳票印刷に要求されるスループット。 業務で必要な帳票の出力時期や枚数を考慮し、どの程度のスループットが必要かを確認する。 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・縮退運転時毎に余裕率を決める。具体的な数値は特定の帳票や機能毎に決めておくことが望ましい。			通常時印刷余裕率	1倍 （余裕無し）	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。				
B.2.5.2							ピーク時印刷余裕率	1倍 （余裕無し）	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。				
B.2.5.3							縮退時印刷余裕率	縮退をしない	通常時の1/2の印刷が出来る	通常時と同様に印刷が出来る									
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。				ー
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。				ー
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。				ー
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。				ー
B.3.3.1			ディスク拡張性	ディスクの拡張性を確認するための項目。 ディスク利用率は、将来の業務量の増加に備え、どれだけディスクに余裕をもたせておくかを確認するための項目。 ディスク拡張性は、物理的もしくは仮想的に、どれだけディスクを拡張できるようにしておくかを確認するための項目。			ディスク利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			○	【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】 ディスクに空きが無い場合、単純増加ファイルの監視等が必要になる。				ー
B.3.3.2							ディスク拡張性	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】 ディスク拡張性がない場合、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。				ー
B.3.4.1			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目。 既存のネットワーク機器を活用する場合は既存ネットワークの要件を確認するために利用する。 ネットワークの帯域については「B.4.1 帯域保証機能の有無」で確認する。			ネットワーク機器設置範囲	無し	フロア内のLAN	同一拠点（ビル）内のLAN	社内複数拠点間の接続（LAN、WAN）	社外拠点との接続						

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
B.3.5.1			サーバ処理能力増強	サーバ処理能力増強方法に関する項目。 将来の業務量増大に備える方法（スケールアップ/スケールアウト）をあらかじめ考慮しておくこと。どちらの方法を選択するかはシステムの特徴によって使い分けることが必要。 スケールアップは、より処理能力の大きなサーバとの入れ替えを行うことで処理能力の増強を行う。 スケールアウトは同等のサーバを複数台用意し、サーバ台数を増やすことで処理能力の増強を行う。			スケールアップ	スケールアップを行わない	一部のサーバのみを対象	複数のサーバを対象				【メトリクス】 あらかじめ余剰リソースを用意しておくことで速やかにスケールアップを行う等、スケールアップの迅速性についても検討する。 また、スケールアップしている状態は、コスト増に繋がる場合があるため、必要に応じてスケールダウンの迅速性についても考慮する。 【レベル1】 オンライントランザクション処理のような更新系の割合が多いシステムでアプリケーションサーバをスケールアップする場合を想定。 【レベル2】 レベル1に加え、DBサーバのスケールアップを追加する場合を想定。				
B.3.5.2							スケールアウト	スケールアウトを行わない	一部のサーバのみを対象	複数のサーバを対象					【メトリクス】 スケールアップと同様、スケールアウトの迅速性についても検討する。 また、必要に応じて、スケールインの迅速性についても検討する。 【レベル1】 Webサーバと負荷分散装置などフロント部分を複数台用意する場合を想定。 【レベル2】 レベル1に加え、バックエンドのサーバを複数台用意する場合を想定。				
B.4.1.1		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度。 伝送遅延時間、パケット損失率、帯域幅をなんらかの仕組みで決めているかを示す。回線の帯域が保証されていない場合性能悪化につながることがある。			帯域保証の設定	無し	プロトコル単位で設定	各サーバ毎に設定	アプリケーションのエンドツーエンドで検証・保証								
B.4.1.2			HWリソース専有の有無	サーバのリソース（CPUやメモリ）を専有するか、共有するかを示す。HWリソースを他のサーバと共有する場合、他のサーバの影響を受けて、性能悪化につながることがある。			HWリソース専有の設定	無し（共有）	有り（専有）										
B.4.2.1			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲。			測定頻度	測定しない	構築当初に測定	運用中、必要時に測定可能	運用中、定常的に測定								
B.4.2.2							確認範囲	確認しない	一部の機能について、目標値を満たしていることを確認	全ての機能について、目標値を満たしていることを確認									
B.4.3.1			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。 特にB2Cシステムなどクライアント数を制限できないシステムで発生する。システムの処理上限を超えることが多いため、Sorry動作を実装し対策する場合が多い。			トランザクション保護	トランザクション保護は不要である	同時トランザクション数の制限機能	同時トランザクション数の制限機能に加え、Sorry動作	独立したSorry動作を行うサーバの設置								
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、システムを稼動させ、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動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動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）	[本番環境] 土曜日、日曜日を除く。（月曜日～金曜日は祝日であっても稼働する。） 9時～18時は事業者と本機関が利用 18時～20時は、本機関のみ利用可能 以降はバッチ稼働時間の設計による。 なお、月1回程度の時間延長を想定 [検証環境] 平日のみの稼働とし運用時間は本番環境と同様 [研修環境] 平日のみの稼働とし運用時間は本番環境と同様	4.15.1. 基本事項
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。				4.15.1. 基本事項

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.1.2.1			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。	○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧					【重複項目】 A.2.6.2。可用性ではデータをどこまで保全するかという観点で、運用ではデータをどこまで復旧させるかという観点で本項目が必要となり、重複項目としている。 【メトリクス】 システムを障害から復旧するためには、データバックアップ以外に、OSやアプリケーションの設定ファイル等を保管するシステムバックアップも必要となることが考えられる。システムバックアップの取得方法や保管方法についても、同時に検討すべきである。 【レベル1】 一部の必要なデータとは、業務継続性の要求を満たすために必要となるようなデータを想定している。				
C.1.2.2						○	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。	2	外部データは利用できない		ー
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	ユーザエラーからの回復	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】 ユーザエラ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		4.9.3. 継続性に係る対策
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。	2	全ステップを自動で行う	・OS、セキュリティパッチ後のバックアップは、手動取得でも可能	4.9.3. 継続性に係る対策
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			4	日次で取得		4.9.3. 継続性に係る対策
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。	4	10年以上有限	・ログファイルは、長期保存対象 ・日々のバックアップサイクルは、一定期間でのラウンド運用	4.9.3. 継続性に係る対策
C.1.2.7					○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ				【重複項目】 A.2.6.1。バックアップ方式は、システムを停止するかどうかの検討が含まれるため、可用性の観点でも考慮する必要があり、重複項目となっている。 【レベル】 オフラインバックアップとは、システム（あるいはその一部）を停止させてバックアップを行う方式、オンラインバックアップとはシステムを停止せず稼働中の状態でバックアップを行う方式を指す。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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。	3	エラー監視（トレース情報を含む）を行う		4.15.2. 情報システムの操作・監視等要件
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）			4	リアルタイム監視（分間隔）		4.15.2. 情報システムの操作・監視等要件
C.1.3.3							システムレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 システムレベルの監視とは、業務アプリケーションも含め、そのシステムを構成する複数のサーバ等の状態確認結果から、システムとして機能する状態にあるかどうかを判断するものである。バックアップの監視やジョブの監視などが該当する。 【レベル】 監視を行う場合には、システムレベルについての監視情報と監視間隔を個別に確認する必要がある。システムが提供するいくつかの機能のうち、重要度の高い一部の機能のみを対象に監視を行うことを想定している。				
C.1.3.4							プロセスレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 プロセスレベルの監視とは、アプリケーションやミドルウェア等のプロセスが正しく機能しているかどうかを判断するものである。主にOSコマンドによるプロセスの情報（死活、CPU使用率、メモリ使用率など）を監視するものを想定している。 【レベル】 監視を行う場合は、プロセスレベルについての監視情報と監視間隔を個別に確認する必要がある。 レベル1の一部とは、システム上で稼動する複数のプロセス（アプリケーションおよびミドルウェア）のうち、重要度の高い一部のプロセスのみを対象に監視を行うことを想定している。				
C.1.3.5							データベースレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 データベースレベルの監視とは、DBMSの機能として提供される情報を確認し、正しく機能しているかを判断するものである。ログ出力内容やパラメータ値、ステータス情報、領域使用率等の監視を想定している。 【レベル】 監視を行う場合は、データベースレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上で稼動する複数のデータベースのうち、重要度の高い一部のデータベースのみを対象に監視を行うことを想定している。				
C.1.3.6							ストレージレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ストレージレベルの監視とは、ディスクアレイ等の外部記憶装置に関して、状態を確認し、正しく機能しているかを判断するものである。OSコマンドによって確認できるディスク使用率等の他、ファームウェアが出力するログ情報などの監視を想定している。 【レベル】 監視を行う場合は、ストレージレベルについての監視情報と監視間隔を個別に確認する必要がある。 レベル1の一部とは、システムに接続される複数のストレージのうち、重要度の高い一部のストレージのみを対象に監視を行うことを想定している。				
C.1.3.7							サーバ（ノード）レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 サーバ（ノード）レベルの監視とは、対象のサーバがOSレベルで正しく機能しているかを判断するものである。ハートビート監視などが該当する。 【レベル】 監視を行う場合は、サーバ（ノード）レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数のサーバ（ノード）のうち、重要度の高い一部のサーバのみを対象に監視を行うことを想定している。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.1.3.8							端末/ネットワーク機器レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 端末/ネットワーク機器レベルの監視とは、クライアント端末やルータ等のネットワーク機器に関して、状態を確認し、正しく機能しているかを判断するものである。ハートビート監視の他、個別のファームウェア等が出力する情報に基づく監視などを想定している。 【レベル】 監視を行う場合は、端末/ネットワーク機器レベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上に存在する複数の端末/ネットワーク機器のうち、重要度の高い一部の端末/ネットワーク機器のみを対象に監視を行うことを想定している。				
C.1.3.9							ネットワーク・パケットレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					【メトリクス】 ネットワーク・パケットレベルの監視とは、ネットワーク上を流れるパケットの情報を確認し、正しく機能しているかを判断するものである。パケットロスやネットワーク帯域の使用率などの監視などを想定している。 【レベル】 監視を行う場合は、ネットワーク・パケットレベルについての監視情報と監視間隔を個別に確認する必要がある。レベル1の一部とは、システム上の複数のネットワーク経路のうち、重要度の高い一部のネットワーク経路のみを対象に監視を行うことを想定している。				
C.1.4.1			時刻同期	システムを構成する機器の時刻同期に関する項目。			時刻同期設定の範囲	時刻同期を行わない	サーバ機器のみ時刻同期を行う	サーバおよびクライアント機器について時刻同期を行う	ネットワーク機器も含めシステム全体で時刻同期を行う	システム全体を外部の標準時間と同期する		○	【レベル4】 システム全体を外部の標準時間と同期する場合、外部との接続に異常が発生した場合にシステム内の時刻同期をどうするかといった設計を行う必要がある。 【運用コストへの影響】 時刻同期を行うことで、複数のサーバ機器が出力するログの順序保証が得られるため、障害調査や監査等の作業コストを下げられる可能性がある。				
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）		ー
C.2.1.2							計画停止の事前アナウンス	計画停止が存在しない	計画停止は年間計画によって確定する	1ヶ月前に通知	1週間前に通知	前日に通知		○	【運用コストへの影響】 計画停止が存在する場合、利用者への通知や運用スケジュールの変更など、イレギュラーな対応が発生する。それらを短時間で実現しなければならないほど、システムの例外処理に対する作り込みを慎重に実施する必要があると考えられ、導入コストが増大すると考えられる。一方、運用コストに関してはその作り込みによって例外処理に対する運用が簡略化されるため減少すると考えられる。				
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。	1	一部の保守作業を自動で実行する	運用コストを含めた全体コスト低減のため、自動化ツールの導入は妨げない。	ー
C.2.2.2							サーバソフトウェア更新作業の自動化	サーバへの更新ファイル配布機能を実装しない	サーバへの更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	サーバへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	サーバへの更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			○	【メトリクス】 サーバソフトウェアとは、サーバ機器のOSやストレージのファームウェア、サーバ機器上で動作するミドルウェアやアプリケーションを指す。 【運用コストへの影響】 サーバへの更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、サーバソフトウェアの更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。				
C.2.2.3							端末ソフトウェア更新作業の自動化	端末への更新ファイル配布機能を実装しない	端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	端末への更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			○	【メトリクス】 端末ソフトウェアとは、クライアント端末のOSやネットワーク機器のファームウェア、クライアント端末上で動作するアプリケーションを指す。 【運用コストへの影響】 端末への更新ファイルの配布や更新処理を自動化するためには、特別なツールを導入したり作り込みを実施する必要があるため導入コストは増大する。一方、端末の更新作業が自動化されることでユーザが運用中に実施すべき作業がなくなり、運用コストは減少する。				
C.2.3.1			パッチ適用ポリシー	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。			パッチリリース情報の提供	ユーザの要求に応じてベンダが受動的にパッチリリース情報を提供する	ベンダが定期的にユーザへパッチリリース情報を提供する	ベンダがリアルタイムに（パッチリリースと同時に）ユーザへパッチリリース情報を提供する									

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.2.3.2							パッチ適用方針	パッチを適用しない	推奨されるパッチのみを適用する	全てのパッチを適用する					【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 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.4.3.2）。				
C.2.3.3							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				【メトリクス】 リリースされるパッチが個別パッチであるか、集合パッチであるかによって選択レベルが変わる場合は、個別に合意する必要がある。 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.2.3.4							パッチ検証の実施有無	パッチ検証を実施しない	障害パッチのみパッチ検証を実施する	障害パッチとセキュリティパッチの両方でパッチ検証を実施する									
C.2.4.1			活性保守	サービス停止の必要がない活性保守が可能なコンポーネントの範囲。			ハードウェア活性保守の範囲	活性保守を行わない	一部のハードウェアにおいて活性保守を行う	全てのハードウェアにおいて活性保守を行う					【メトリクス】 ハードウェア活性保守とは、システムを停止せずにハードウェア交換やファームウェア更新といった保守作業を実施することである。 【レベル1】 一部のハードウェアとは、特定のサーバやストレージのみ活性保守を可能とするようなケースを指す。				
C.2.4.2							ソフトウェア活性保守の範囲	活性保守を行わない	一部のソフトウェアにおいて活性保守を行う	全てのソフトウェアにおいて活性保守を行う					【メトリクス】 ソフトウェア活性保守とは、システムを停止せずにOSやミドルウェア、アプリケーションのパッチ適用を実施することである（例：マルチサーバ環境におけるローリングアップグレードなど）。 【レベル1】 一部のソフトウェアとは、特定のソフトウェアのみ活性保守を可能とするようなケースを指す。				
C.2.5.1			定期保守頻度	システムの保全のために必要なハードウェアまたはソフトウェアの定期保守作業の頻度。			定期保守頻度	定期保守を実施しない	年1回	半年に1回	月1回	週1回	毎日						
C.2.6.1			予防保守レベル	システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守。			予防保守レベル	予防保守を実施しない	定期保守時に検出した予兆の範囲で対応する	（定期保守とは別に）一定間隔で予兆検出を行い、対応を行う	リアルタイムに予兆検出を行い、対応を行う								
C.3.1.1		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧				【重複項目】 A.4.1.1。復旧作業は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目であるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 選定したレベルに応じて、ユーザ側・ベンダ側それぞれの体制や権限の整理を実施する必要がある。 【レベル】 自作ツールを利用するケースは手作業に含む。 復旧用製品とは、バックアップ・リカバリを行う製品を指す。復旧用製品による復旧を行う場合、どこまで自動化するか（自動リカバリー機能充足率など）を定義するケースもあるが、可用性としては、復旧用製品を使用するかしないかでギャップが発生するため、この観点でレベルを検討する。	3	復旧用製品＋業務アプリケーションによる復旧		ー
C.3.1.2					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要					【重複項目】 A.4.1.2。代替業務運用の範囲は、可用性の復旧目標（RTO/RPO）を検討するうえで必要な項目でもあるため、可用性と運用・保守性の両方に含まれている。 【メトリクス】 代替業務運用とは、障害によりシステムが復旧不可能となった場合に、代替業務でカバーすることが可能な運用手段（代替機あるいは人手による運用）を指す。	1	一部の業務について代替業務運用が必要	システム復旧後、当日分のデータについては再入力を想定	ー
C.3.2.1			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目。			障害復旧自動化の範囲	障害復旧作業は全て手動で実施する	一部の障害復旧作業を自動化する	全ての障害復旧作業を自動化する				○	【レベル1】 一部の障害復旧作業とは、特定パターン（あるいは部位）の障害復旧作業に関してのみ自動化を行うようなケースを指す。 【運用コストへの影響】 障害復旧作業を自動化するためには、障害のパターン毎に複雑な判断を行うスクリプトを作成する必要があり開発コストが増大する。一方、障害発生時の復旧作業が迅速化され、ミスも少なくなるため運用コストは減少する。				
C.3.3.1			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目。			対応可能時間	ベンダの営業時間内（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					【メトリクス】 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。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.3.3.2							駆けつけ到着時間	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		【メトリクス】 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。				
C.3.3.3							SE到着平均時間	SEの駆けつけ無し	SE到着が異常検知から数日中	SE到着が異常検知からユーザの翌営業日中	SE到着が異常検知からユーザの翌営業開始時まで	SE到着が異常検知から数時間内	SEが常駐		【メトリクス】 システム異常を検知してからSEが到着するまでの平均時間。				
C.3.4.1			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法。			保守部品確保レベル	確保しない	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保する					【メトリクス】 当該システムに関する保守部品の確保レベル。				
C.3.4.2							予備機の有無	予備機無し	一部、予備機有り	全部、予備機有り									
C.4.1.1		運用環境	開発用環境の設置	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。 【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。	1	運用環境の一部に限定した開発環境を設置する		4.11.2. 構築すべき環境
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。 【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。	2	専用の試験用環境を設置する		4.11.2. 構築すべき環境
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。	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		4.14. 教育に関する事項
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。	2	遠隔地でリモート監視を行う		ー
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。	2	任意のリモート操作を行う		ー
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。	1	社内の外部システムと接続する		3.5.1. 連携システム

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.4.5.2							監視システムの有無	監視システムは存在しない	既存監視システムに接続する	新規監視システムに接続する					【レベル2】 新規監視システムに接続とは、当該システムに対する監視機能の新規構築が要件定義範囲に含まれていることを意味している。				
C.4.5.3							ジョブ管理システムの有無	ジョブ管理システムは存在しない	既存ジョブ管理システムに接続する	新規ジョブ管理システムに接続する					【レベル2】 新規ジョブ管理システムに接続とは、当該システムに対するジョブ管理機能の新規構築が要件定義範囲に含まれていることを意味している。				
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（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）			○	【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。	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）		ー
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（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）			○	【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。	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）		ー
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。	3	10年以上		ー
C.5.4.1			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目。			メンテナンス作業役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施									
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。			一次対応役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施									
C.5.6.1			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目。			ベンダ側常備配備人数	常駐しない	1人	複数人									
C.5.6.2							ベンダ側対応時間帯	対応無し	ベンダの定時時間内（9～17時）	夜間のみ非対応（9～21時）	引継ぎ時に1時間程度非対応有り（9～翌8時）	24時間対応							
C.5.6.3							ベンダ側対応者の要求スキルレベル	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている							
C.5.6.4							エスカレーション対応	指定無し	オンコール待機	拠点待機	現地待機				【メトリクス】 障害発生時にエスカレーション対応が必要となるISV/IHV製品に関してエスカレーション先の有識者の待機方法について確認する。				
C.5.7.1			導入サポート	システム導入時の特別対応期間の有無および期間。			システムテスト稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上							

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
C.5.7.2							システム本稼働時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上				4	1ヶ月以上	システム本稼働時に発生した問題の早期解決を図るため、導入から一連の業務サイクルが完了する期間のうち1ヶ月程度を特別対応期間とすること。 当システムに関連する初回イベント時には特別体制を構築することを望む。	ー
C.5.8.1			オペレーション訓練	オペレーション訓練実施に関する項目。			オペレーション訓練実施の役割分担	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施								
C.5.8.2							オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施				【レベル】 通常運用とは、システム基盤に対する通常時の運用（起動・停止等）にかかわる操作を指す。保守運用とは、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）にかかわる操作を指す。				
C.5.8.3							オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催									
C.5.9.1			定期報告会	保守に関する定期報告会の開催の要否。			定期報告会実施頻度	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上		【メトリクス】 障害発生時に実施される不定期の報告会は本メトリクスには含まない。	4	月1回		ー
C.5.9.2							報告内容のレベル	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	障害および運用状況報告に加えて、改善提案を行う					3	障害および運用状況報告に加えて、改善提案を行う		ー
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	内部統制対応について規定しない	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。	1	既存の社内規定に従って、内部統制対応を実施する		ー
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ついて規定しない	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ついて規定しない		4.15.5.1. ヘルプデスク
C.6.3.1			インシデント管理	業務を停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目。			インシデント管理の実施有無	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する					【メトリクス】 ここでは、当該システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の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。				
C.6.4.1			問題管理	インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施するかどうかに関する項目。			問題管理の実施有無	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する					【メトリクス】 ここでは、インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の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。				
C.6.5.1			構成管理	ハードウェアやソフトウェアなどのIT環境の構成を適切に管理するためのプロセスを実施するかどうかに関する項目。			構成管理の実施有無	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する					【メトリクス】 ここでは、リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の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。				
C.6.6.1			変更管理	IT環境に対する変更を効率的に管理するためのプロセスを実施するかどうかに関する項目。			変更管理の実施有無	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する					【メトリクス】 ここでは、ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の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。				
C.6.7.1			リリース管理	ソフトウェア、ハードウェア、ITサービスに対する実装を管理するためのプロセスを実施するかどうかに関する項目。			リリース管理の実施有無	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する					【メトリクス】 ここでは、承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の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。				
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	2024年3月頃を想定	4.13. 移行に関する事項

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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		【メトリクス】 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。	0	制約無し（必要な期間の停止が可能）		4.13. 移行に関する事項
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		4.13. 移行に関する事項
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の程度。		○	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		ー
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		ー
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		ー
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）。		○	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		4.13. 移行に関する事項
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					【メトリクス】 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。	2	移行先と形式が異なる		4.13. 移行に関する事項
D.4.2.1			移行媒体	移行対象となる媒体の量と移行時に必要となる媒体種類数。			移行媒体量	移行対象無し	10本未満（1TB未満）	1000本未満（1PB未満）	1000本以上（1PB以上）								
D.4.2.2							移行媒体種類数	移行対象無し	1種類	2種類	3種類	4種類	5種類以上		【メトリクス】 移行する際に使用しなければならない媒体の種類を計数する（例えば、テープ、ディスク、紙の伝票類、など）。 また、ネットワーク接続によるデータ転送も媒体種類として含む。				
D.4.3.1			変換対象（DBなど）	変換対象となるデータの量とツールの複雑度（変換ルール数）。			変換データ量	変換対象無し	1TB未満	1PB未満	1PB以上								
D.4.3.2							移行ツールの複雑度（変換ルール数）	移行ツール不要または既存移行ツールで対応可能	変換ルール数が10未満の移行ツールの複雑度	変換ルール数が50未満の移行ツールの複雑度	変換ルール数が100未満の移行ツールの複雑度	変換ルール数が100以上の移行ツールの複雑度							
D.5.1.1		移行計画	移行作業分担	移行作業の作業分担。			移行のユーザ/ベンダ作業分担	全てユーザ	ユーザとベンダと共同で実施	全てベンダ					【メトリクス】 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、ユーザとベンダで取り交わしを行うことが望ましい。具体的内容については、「F.1.1.1 構築時の制約条件」にて確認する。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダ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。				
D.5.2.1			リハーサル	移行のリハーサル（移行中の障害を想定したリハーサルを含む）。			リハーサル範囲	リハーサル無し	主要な正常ケースのみ	全ての正常ケース	正常ケース＋移行前の状態に切り戻す異常ケース	正常ケース＋システム故障から回復させる異常ケース							

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
D.5.2.2							リハーサル環境	リハーサル無し	本番データ使用可能	本番データ使用不可					【レベル】 本番データを使用することによる情報漏えい等のセキュリティリスクは、「F.1.1.1 構築時の制約条件」にて判断し、ここではリハーサル環境に限定して判断する。				
D.5.2.3							リハーサル回数	リハーサル無し	1回	2回	3回	4回	5回以上						
D.5.2.4							外部連携リハーサルの有無	無し	有り（外部接続仕様の変更無し）	有り（外部接続仕様の変更有り）					【メトリクス】 外部システムとの接続仕様が変更になる場合、システム移行リスクを軽減するために新システムでは新旧両接続仕様をサポートすることがある。その場合には、両接続仕様を確認するための外部連携リハーサルを計画すること。 【レベル】 外部連携リハーサル有りの場合、そのリハーサル対象の外部システムとリハーサル範囲、環境、回数について規定すること。				
D.5.3.1			トラブル対処	移行中のトラブル時の対応体制や対応プラン等の内容。			トラブル対処の規定有無	規定無し	対応体制のみ規定有り	対応体制と対応プランの規定有り					【レベル】 トラブル対処の規定有りの場合、その対応体制や対応プランの規定内容について確認すること。				
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						【メトリクス】 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。	1	有り		4.10.3.1. セキュリティ機能
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					【メトリクス】 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。	2	開発範囲		4.10.3.1. セキュリティ機能
E.3.1.1		セキュリティ診断	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						【メトリクス】 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		4.10.3.1. セキュリティ機能
E.3.1.2						○	Web診断実施の有無	無し	有り						【メトリクス】 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		4.10.3.1. セキュリティ機能
E.3.1.3							DB診断実施の有無	無し	有り						【メトリクス】 DB診断とは、データベースシステムに対して行うセキュリティ診断のことを言う。 【レベル1】 DB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。				
E.4.1.1		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目。 セキュリティリスクの見直しには、セキュリティホールや脆弱性、新たな脅威の調査等が含まれる。			セキュリティリスク見直し頻度	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施					【レベル】 セキュリティに関するイベントとは、重要な脅威や脆弱性の発見、ウィルス感染、不正侵入、DoS攻撃、情報漏えいなどの情報セキュリティに関するインシデントのことを指す。	2	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施		ー

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
E.4.1.2							セキュリティリスクの見直し範囲	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	システム全体						2	システム全体		ー
E.4.2.1			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目。 また、検討するにあたり、発見された脅威についての対応範囲について明らかにする。			運用開始後のリスク対応範囲	対応しない	重要度が高い資産に関連する、あるいは、外接部分の脅威に対応	洗い出した脅威全体に対応						2	洗い出した脅威全体に対応		ー
E.4.2.2							リスク対策方針	無し	有り						【レベル1】 リスク対応方針がある場合は、どのような対策を実施するのかを確認する必要がある。	1	有り		ー
E.4.3.1			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。			セキュリティパッチ適用範囲	セキュリティパッチを適用しない	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						2	システム全体		ー
E.4.3.2							セキュリティパッチ適用方針	セキュリティパッチを適用しない	緊急性の高いセキュリティパッチのみ適用	全てのセキュリティパッチを適用						1	緊急性の高いセキュリティパッチのみ適用		ー
E.4.3.3							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				【レベル】 セキュリティパッチを適用するまでの脅威等にさらされている期間は、監視強化や暫定対策の実施を検討する。 【レベル3】 パッチが出荷されてから適用するまでの期間について検討することが望ましい。パッチ検証を実施する場合、環境準備等を含め、パッチ適用までに期間を要することを考慮する。	2	定期保守時に実施		ー
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				【メトリクス】 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。	3	複数回、異なる方式による認証		4.10.3.1.1. 主体認証機能
E.5.1.2							管理権限を持たない主体の認証	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					3	複数回、異なる方式による認証		ー
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					【メトリクス】 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		ー
E.5.2.2							物理的な対策による操作制限度	無し	必要最小限のハードウェアの利用や操作のみを許可						【メトリクス】 セキュリティゲート等のファシリティによるサーバルームへの入退室管理、情報の保管場所や、サーバ等に対する施錠、USBやCD-RWの入出力デバイスの制限等のための物理的な対策実施を示す。				
E.5.3.1			管理方法	認証に必要な情報（例えば、ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報）の追加、更新、削除等のルール策定を実施するかを確認するための項目。			管理ルールの策定	実施しない	実施する							1	実施する		ー

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
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。	2	重要情報を暗号化		4.10.3.1.3. データの暗号化機能
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。	2	重要情報を暗号化		4.10.3.1.3. データの暗号化機能
E.6.1.3							鍵管理	無し	ソフトウェアによる鍵管理	耐タンパデバイスによる鍵管理					【レベル】 ソフトウェアによる鍵管理とは、秘密鍵情報に対し、ソフトウェアの設定等によりアクセス制御を実施するような管理のことである。 耐タンパデバイスによる鍵管理とは、ICカードのような、物理的な仕掛により、攻撃への耐性を高めた専用デバイスによる管理のことである。これにより、鍵情報の改竄や漏洩といった脅威に対して、より厳密に管理することができる。				
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						【メトリクス】 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		4.10.3.1.6. ログ管理機能
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			4	10年以上有期		4.15.4.1. ログ出力・蓄積・監視要件
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					【メトリクス】 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メトリクス。	2	システム全体		4.15.4.2. ログ収集要件
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					【メトリクス】 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メトリクス。	2	システム全体		4.15.4.2. ログ収集要件
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					【メトリクス】 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。	2	システム全体		4.15.4.2. ログ収集要件

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
E.7.1.6							確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認				【レベル3】 常時確認とは、常に不正なアクセス等を監視し、即座に対応可能な状態を意味する。 自動検知システムを導入し、不正検知時にメール等で通知する仕組みの導入は、セキュリティに関するイベントの発生時に実施（随時）に含まれる。	2	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施		ー
E.7.2.1			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目。			デジタル署名の利用の有無	無し	有り										
E.7.2.2							確認間隔	無し	セキュリティに関するイベントの発生時に実施（随時）	セキュリティに関するイベントの発生時に実施（随時） ＋ 定期的に実施	常時確認							
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際には、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		4.10.3.1.2. 通信の暗号化機能
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					【メトリクス】 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。	2	システム全体		4.15.2. 情報システムの操作・監視等要件
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		ー
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア（ウィルス、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、ウィ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						2	システム全体		4.10.3.1.5 ウィルス対策機能
E.9.1.2							リアルタイムスキャンの実施	実施しない	実施する						【レベル1】 リアルタイムスキャンは、例えば、以下のようなタイミングで実施する。実施する際は実施するタイミングを検討する必要がある。 ・ファイルサーバへデータをコピーするタイミング ・メールサーバがメールを受信したタイミング ・ファイルへの入出力処理が実行される前 等	1	実施する		ー
E.9.1.3							フルスキャンの定期チェックタイミング	無し	不定期（フルスキャンを行えるタイミングがあれば実施する）	1回／月	1回／週	1回／日				1	不定期 （フルスキャンを行えるタイミングがあれば実施する）		ー
E.10.1.1		Web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						【メトリクス】 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		ー
E.10.1.2						○	WAFの導入の有無	無し	有り						【メトリクス】 WAFとは、Web Application Firewallのことである。	1	有り		ー

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
E.11.1.1		セキュリティインシデント対応/復旧	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。			セキュリティインシデントの対応体制	無し	有り						【メトリクス】 セキュリティインシデント発生時の対応以外にも、インシデント対応マニュアルの整備や、システムの関係者に対するセキュリティ教育を実施する。 【レベル0】 セキュリティインシデント発生の都度、インシデント対応体制を構築する場合も含まれる。 【レベル1】 新たに対応体制を構築する他に、ユーザ企業内のCSIRTを利用する場合や、外部のセキュリティ対応サービスを利用する場合も含まれる。	1	有り		ー
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）					【メトリクス】 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生じる。 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。	2	制約有り(全ての制約を適用)		ー
F.1.2.1			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）						2	制約有り(全ての制約を適用)		ー
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。	1	上限が決まっている		要件定義書別紙02_主要業務量一覧
F.2.2.1			クライアント数	システムで使用され、管理しなければいけ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						1	上限が決まっている		要件定義書別紙02_主要業務量一覧
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。	1	複数拠点		2. 業務要件の定義
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対応が必要となる。	4	国内		2. 業務要件の定義
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		ー
F.2.6.1			システム利用範囲	システム利用者が属する属性の広がり。			システム利用範囲	部門内のみ	社内のみ	社外（BtoB）	社外（BtoC）								
F.2.7.1			複数言語対応	システム構築の上で使用が必要、またはサービスとして提供しなければならない言語。扱わなければならない言語の数や各言語スキル保持者へのアクセシビリティを考慮。			言語数	数値などのみ扱う	1	2	5	10	100		【レベル】 言語数だけでなく、別途、言語の難易度も併せて検討することが必要である。 また、通貨単位なども考慮しておく必要がある。 【レベル0】 数値データなどのみを扱うとは、人に対するプレゼンテーション機能を想定せず、マシン間でのインターフェースを扱うようなシステムを想定している。例えば、GWシステムなどである。				
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		ー
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		ー

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
F.3.3.1			電磁干渉	提供するシステムに使用する製品について、VCCIなどの機器自身が放射する電磁波をある一定以下のレベルに抑える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	VCCI ClassA取得	VCCI ClassB取得									
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）		【メトリクス】 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有り）。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。				―
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					【メトリクス】 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。				―
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					【メトリクス】 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。				―
F.4.2.3							並行稼働スペース(移行時)	専用スペースの確保が可能	共用スペースの確保が可能	確保不可					【メトリクス】 構築時に、まだ本番運用で用いるスペースが使用できない場合は、構築時のスペースおよび移設に関しても考慮すること。更に、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2】 並行稼働有りの場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.4.3がある。				
F.4.2.4							設置スペースの拡張余地	十分な拡張余地有り	一部制約有り(既製品で対応できるレベル)	制約有り(特注対応や工事が必要)					【メトリクス】 設置スペースの拡張余地には、フロアに直接置くだけでなくラックの制約や床荷重なども含まれる。				
F.4.3.1			重量	建物の床荷重を考慮した設置設計が必要となることを確認する項目。低い床荷重の場合ほど、設置のための対策が必要となる可能性が高い。			床荷重	2,000Kg/㎡以上	1,200Kg/㎡	800Kg/㎡	500Kg/㎡	300Kg/㎡	200Kg/㎡	○	【レベル】 床が耐えられる荷重でレベル化。耐荷重が大きいほど設置に関する制約が少ない。 【運用コストへの影響】 床荷重が高い場合、副次的に高密度な実装となり、高ラック位置での保守作業などが必要になる場合がある。				
F.4.3.2							設置対策	不要	荷重を分散するための資材(鉄板など)を配備する	ラック当りの重量を制限して、分散構成を採る	設置環境固有の条件(梁の場所など)を考慮して、設置設計を行う								
F.4.4.1			電気設備適合性	ユーザが提供する設置場所の電源条件(電源電圧/電流/周波数/相数/系統数/無停止性/必要工事規模など)と導入システムの適合性に関する項目。同時に空調についても評価対象とする。また、移行時の並行稼動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。			供給電力適合性	現状の設備で特に制限無し	電源工事は必要だが、分電盤改造など二次側の工事のみで対応可能	電源工事は必要だが、一次、二次とも工事可能	工事などができず、規模に対して容量が少し足りない	まったく対応できず、設置場所を再考する必要がある							
F.4.4.2							電源容量の制約	制約無し(必要な電源容量の確保が可能)	制約有り(既製品で対応できるレベル)	制約有り(カスタマイズや工事が必要)									
F.4.4.3							並行稼働電力(移行時)	全面的に確保が可能	部分的に確保が可能	確保が困難					【レベル2】 移行時に並行稼働が必要な場合には、別途対策を検討すること。関係項目に D.1.1.3、F.4.2.3がある。				
F.4.4.4							停電対策	無し	瞬断(10ms程度)	10分	1時間	1日間	1週間		【レベル1】 UPS, CVCFなど電源安定化の対策を検討する。				
F.4.4.5							想定設置場所の電圧変動	±10%以下	±10%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS, CVCFなど電源安定化の対策が必要となる。				
F.4.4.6							想定設置場所の周波数変動	±2%以下	±2%を超える						【レベル1】 機材の動作条件を逸脱する場合には、UPS, CVCFなど電源安定化の対策が必要となる。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム			要件定義書記載箇所
								0	1	2	3	4	5			選択レベル		備考	
F.4.4.7							接地	接地不要	接地が必要	専用接地が必要									
F.4.5.1			温度（帯域）	システムが稼働すべき環境温度の帯域条件。周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。			温度（帯域）	対策不要	16度から32度（多くのテープ装置の稼働可能条件）	5度から35度（多くの機器の稼働可能条件）	0度～40度	0度～60度	-30度～80度		【メトリクス】 温度勾配は10℃/h程度以下に抑えることも併せて考慮する。また、レベル2以上の環境では非稼働時の確認も別途必要である。 【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境温度が0～20度で変動している環境であれば、それを満たすレベルの中で一番低いレベル3となる。				
F.4.6.1			湿度（帯域）	システムが稼働すべき環境湿度の帯域条件。周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。			湿度（帯域）	対策不要	45%～55%	20%～80%	0%～85%	結露無し条件のみ			【レベル】 機器が稼働している状態での周囲環境の変動範囲でレベルを選択する。例えば、周囲環境湿度が20～50%で変動している環境であれば、それを満たすレベルの中で一番低いレベル2となる。				
F.4.7.1			空調性能	システムを稼働させるのに十分な冷却能力を保持し、特定のホットスポットが存在する場合にはそれを考慮した冷気供給を行える能力。			空調性能	十分な余力有り	ホットスポットなどへの部分的な対策が必要	能力が不足しており、対策が必要					【メトリクス】 必要に応じて塵芥や有害ガスへの対応なども考慮する。				
F.4.7.2							空調設備の制約	制約無し（必要な空調の確保が可能）	制約有り（既製品で対応できるレベル）	制約有り（カスタマイズや工事が必要）									
F.5.1.1		環境マネージメント	環境負荷を抑える工夫	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。			グリーン購入法対応度	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									
F.5.1.2							同一機材拡張余力	無し	2倍	4倍	10倍	30倍	100倍以上		【メトリクス】 既設機材を廃棄することなく、単純に追加で拡張可能であることを意味する（契約上は追加であっても実際には機材全体を置き換えてしまい全廃棄が発生するようなものは対象外となる）。製造エネルギー、廃棄物量までを考慮する。 【レベル】 数倍程度まではスケールアップ主体、それ以上はスケールアウト主体での対応となると考えられる。				
F.5.1.3							機材の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実質的なハードウェア入れ替え期間と規定している。基本的に長期に渡って使用することが望ましいが、あまりにも長期過ぎると性能向上や省電力技術の進歩などの恩恵が受けられなくなることにも注意が必要である。 【運用コストへの影響】 ライフサイクルの短い機材を使用すると、頻繁な更新が必要となるため、運用コストが増大する懸念がある。				
F.5.2.1			エネルギー消費効率	本来はシステムの仕事量をそのエネルギー消費量で除した単位エネルギー当りの仕事量のこと。ただし、汎用的な仕事量の定義が存在しないため、効率を直接求めることは困難である。また、同じ仕事を行う別のシステムも存在しないことが多いため、比較自体も困難である。このため、エネルギー消費効率に関しては、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。なお、電力エネルギーを前提とするシステムでは、消費電力≒発熱量である。 また、システムの仕事量の視点ではなく、データセンターのエネルギー効率を示す指標にPUE(Power Usage Effectiveness)や、DPPE(Datacenter Performance Per Energy)などがある。			エネルギー消費の目標値	目標値無し	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る				○	【レベル0】 電源設備などとの整合性の再確認が必要である。 【レベル2】 レベル1の目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合がある。				
F.5.3.1			CO_2排出量	システムのライフサイクルを通じて排出されるCO_2の量。ただし、単純なCO_2排出量でレベル化するのは困難であるため、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。			CO_2排出量の目標値	目標値の設定不要	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る				○	【メトリクス】 運転時のCO_2排出量は基本的に電力消費量とリンクする形になる。これに生産・廃棄におけるCO_2排出量を加えたものがライフサイクル全体での排出量となる。 【レベル0】 目標値の設定不要とした場合、CSRなどとの整合性の再確認が必要である。 【レベル2】 レベル1の目標値達成に止まらず、更に厳しい基準へのオプション要望があることを示す。 【運用コストへの影響】 低いレベルで合意した場合、新法令の制定などで運用後に対応が必要となる場合がある。				
F.5.4.1			低騒音	機器から発生する騒音の低さの項目。特にオフィス設置の場合などには要求度が高くなる傾向がある。また、データセンターなどに設置する場合でも一定以上の騒音の発生は労働環境として問題となることがある。			騒音値	対策不要	87dB(英国RoSPAの騒音基準による防音保護具の使用も考慮に入れた許容限界値)以下	85dB(英国RoSPAの騒音基準による第2アクションレベル)以下	80dB(英国RoSPAの騒音基準による第1アクションレベル)以下	40dB(図書館レベル)以下	35dB(寝室レベル)以下	○	【運用コストへの影響】 低いレベルで合意した場合、労働環境との整合性の再確認が必要である。				

項番	大項目	中項目	小項目	小項目説明	重複項目	重要項目	メトリクス（指標）	レベル						運用コストへの影響	備考	本システム		要件定義書記載箇所
								0	1	2	3	4	5			選択レベル	備考	

※ 　は現段階では定めていない項目