

非機能要求グレード2018 改訂情報 ~初版との差異~

2018年4月25日

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

改訂の目的

情報システムの開発では、業務機能に関する要求以外のいわゆる「非機能要求」について、ステークホルダ間の認識の行き違いに気づかないまま開発が進んでしまうことがあります。「非機能要求グレード」は、このような状態を防止することを目的とし、重要な項目から段階的に詳細化しながら非機能要求の確認を行うツール群です。

IPA/SECでは2010年4月に、非機能要求グレードの初版を公開しました。 非機能要求グレードのダウンロード数は、初版公開から数年を経ても一定の水準を維持しており、普及が進んでいます。その一方で、新たなセキュリティ脅威の台頭や、システム基盤技術の進展により、初版公開当時から、非機能要求に変化が生じてきています。

非機能要求の定義漏れを防止するため、非機能要求グレードにおける、これまでのスコープは維持したまま、これらの非機能要求の変化に追従するかたちで、非機能要求グレードの改訂を行いました。

改訂の対象

初版公開以降における社会や技術の変化に伴って、非機能要求が変化した、セキュリティと仮想化に関する要求を、主な改訂対象としました。

代表的な社会や技術の変化

HW性能の 向上 サイバー攻撃の 高度化 OSSの コモディティ化 仮想化技術の 成熟 IoTやAIや モバイルの普及 クラウドの 普及 システムの グローバル化

改訂対象① セキュリティに関する要求

標的型攻撃等の出現により、サイバー攻撃を完全に防御することは困難になってきました。そのため、防御しきれずに侵入されることを前提とした新しいセキュリティの考え方や、ログの相関分析といった新しいセキュリティ対策について、非機能要求として定義できるように改訂しました。

また、システムのグローバル化が進んだことにより、 要求を決める段階で、日本以外の国や地域の法令な ども把握することが必要不可欠になり、この点につ いても非機能要求を定義できるようにしました。

改訂対象② 仮想化に関する要求

クラウドの中核技術のひとつである仮想化技術が成熟したことによって、ハードウェアリソースを柔軟に振り分けて管理することができ、また、スケールアウトなどの拡張が迅速に行えるようになってきました。このような、仮想化によって実現可能になった要求について、非機能要求として定義できるように改訂しました。

あわせて、一部のメトリクスなどについて、"スロット"などのような物理的な表現になっているため、仮想化が浸透した現在では表現が相応しくなくなったものがあり、それらについては表現を見直しました。

改訂の一例

従来の非機能要求グレードの全体236メトリクスに対し、新規追加が2メトリクス、既存項目に何らかの修正を施したものは20メトリクスとなります。一例を以下に示します。 なお、改訂箇所を赤字にした「活用シート」を付録に示します。

セキュリティに関する改訂の一例

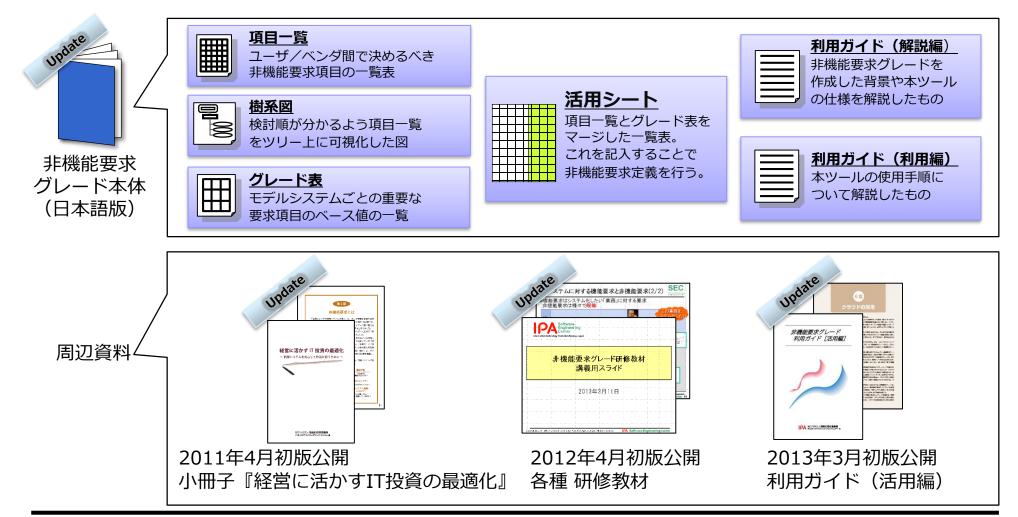
項番	区分	具体的箇所	改訂內容
1	セキュリティ	E.11.1.1 セキュリティインシデ ントの対応体制 ※新規メトリクス	標的型攻撃のような、完全防御することが事実上不可能な攻撃が出てきている。そのため、セキュリティインシデントは発生するものという見地から、早期検出、早期対処をするためのインシデントレスポンスチームの常設要否を決めるための、新規メトリクスを追加した。
2	セキュリティ	E.1.1.1 順守すべき社内規程、 ルール、法令、ガイド ライン等の有無	業務だけでなく、パブリッククラウド等の普及により、システム基盤の グローバル化も進んでいる。それに伴い、例えばEU一般データ保護規則 (GDPR)のような、国や地域特有の法令やガイドラインを忘れずに順 守するよう、既存メトリクスの記載を拡充した。

仮想化に関する改訂の一例

項番	区分	具体的箇所	改訂内容
1	性能・拡張性	B.4.1.2 HWリソース専有の設 定 ※新規メトリクス	複数の論理サーバ間でCPU等のハードウェアリソースを共有し融通しあ うオーバコミットによって、リソースをより有効活用することも可能に なってきた。このようなオーバコミットの採否を決めるための、新規メ トリクスを追加した。
2	可用性	A.2.5.3 冗長化(ディスク)	従来の非機能要求グレードでは、RAID1やRAID5といったRAIDレベルでストレージの冗長性が表現されていた。仮想化技術をベースにした分散ストレージなど、RAID以外の冗長化も存在しており、従来の記載が合理的ではなくなってきたため、既存メトリクスの記載を見直した。

改訂した成果物一覧

主要な改訂は「非機能要求グレード本体」です。本体のうちの利用ガイド(解説編、利用編)、および周辺資料の利用ガイド(活用編)や小冊子、各種研修教材は、メトリクスの総数など、改訂内容と整合させる必要がある部分のみを更新しました。



(付録)

項番 大 項番 人 項	項目				./ I	167			ベル			運用コ		TA	り影響が殆ど無いシステム	1 社会的	影響が限定されるシステム	1 社会的家	影響が極めて大きいシステム
A.1.1.1 可用性		中項目 小項目	小項目説明	複 項 目	要 ダ 項 (指 目	i標) () 1	2	3	4		ストへ の影 響	備考	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
	月性 総	継続性 運用スケジル	1- システムの稼働時間や停止運用に関する情報。	<u>-</u>	運用時常)	請問(通 規定報	無し 定時内 (9時~1 時)	夜間のみ 7 停止 (9時~21 時)	の停止有	(9時~翌	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。	停止	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	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	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
									14,1024,7				【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】		[+] 24時間無停止やリブート処理等の短時間の停止のみを考える場合		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		場合
													()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。	b					
A.1.1.2					運用時定日)	計間(特 規定領	無し 定時内 (9時~1 時)		の停止有	(9時~翌	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。		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	2 夜間のみ 停止 (9時~21	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		 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
				0	0			Hij/	朝8時)	分)			【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。		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	H-1] /	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		存在する場合
A.1.1.3					計画停有無	有り(亨止 計画停』 運用 有り(運) ジュー スケジュ	用┃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	有り(運	事前の合意があれば、停止は可能。	1 計画停止 有り(運 用スケ	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。	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。
				0	0		変更 ルの変す不可)					0	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。	ジュール の変更 可)	[+] 運用時間外での停止だけで対 応可能な場合	ジュール	回的な停止は可能。 [-] 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		[-] 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。	Ç	対象業囲		向け 内部向け ・系 オンライン 系業務			外部向け オンライン 系業務			【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】	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	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	オンライ	外部とのリアルタイムでの処理が 主要業務であり、外部向けオンラー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。
					0								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。		(+) 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		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		[-] 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 時間	ス切替 24時 上	間以 24時間 満 満	大 大 2時間未満 1	高 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。		外部向けの業務はなく、1日程度の 中断であれば許容できる。 [-] 障害時の対策を必要としない場		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。	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。
					0							0	【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。		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)		[+] 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)		[-] 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					業務継要求度	業務何	寺の 単一障害 亭止 時は業務 字す 停止を討 容せず、	务 時でも	2				【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	時は業務 停止を許	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	時でも サービス	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	時でも サービス	二重障害でも業務継続が前提となる。 る。
					0		処理を総続させる	≝ の規定内					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。	処理を継	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		での業務停止を許容できる場合	の規定内で継続する	
A.1.3.1			準 業務停止を伴う障害が発生した際、何をどこり で、どれ位で復旧させるかの目標。	i.s	RPO([旧地点		下要 5営業日 の時点 (週次バ		時点 ソ (日次バッ	,			【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。	前の時点	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。		データの損失は許容できないた め、障害発生時点までの復旧が原 則。
					0		らの復旧	らの復旧) アーカイフ からの復 旧)	Ĵ			【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。	プからの 復旧)	[-] データを持たず、復旧が不要な場合 [+] 日次のバックアップからの復旧でないと、データ損失の影響が大きい場合	プ+アーカ イブから の復旧)	[-] 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)	プ+アーカ イブから	
A.1.3.2					RTO(E 旧時間		日以 1営業日 内	以 12時間以 内	6時間以内	7 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。		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	内	なるべく早く復旧する。
A.1.3.3					RLO(E 旧レベ		ーム 特定業務 日 のみ	务 全ての業 発	:					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る。		注: 未務停止の影響が入さい場合	2 全ての業	全ての業務が稼働していないと影響がある。
					0	· · · / · / · · · · · · · · · · · · · ·		320					【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。		[+] 業務毎に影響を切り離せない 場合		[-] 影響を切り離せる業務がある場合		[-] 影響を切り離せる業務がある場合
A 1 4 1			淮 十担塔巛宝が&井口・呶 じんはったにたい		2.→-	/. 声問 李丽-	不要 数ヶ月以	l, - N	`阻胆!\!	20 N + 1-	1000		【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 ***, □ \\\\	データの指生はもて和英語ので	2 _ '田田! い	十担増巛宝吐は 児笠ナフデ と	4 20 N +	ニノつニノンの名にナネホー、・
A.1.4.1			準 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	自には	目標	△丹周 井開 ′		人 一ヶ月以 引 内に再開			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。	内に再開	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 [+] 業務停止の影響が大きい場合		大規模災害時は、保管するデータからの復旧により業務を再開する。 [-] 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		ライノラインの復旧を考慮し、システムとして最大限の回復に努める。 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合

社会的影響が限定されるシステム

選択時の条件

選択レベル

社会的影響が極めて大きいシステム

選択時の条件

選択レベル

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。

社会的影響が殆ど無いシステム

選択時の条件

1年間で数時間程度の停止を許

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

					重重				レ	ベル			運用□		
項番	大項目	中項目	小項目	小項目説明	重複項目	リントリクス (指標)	0	1	2	3	4	5	運用コ ストへ の影 響	備考	選:
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%・・・・・ 52.6分 99.999%・・・・・ 5.26分	2
														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%	
.2.1.1		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		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。	
														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	ンポーネン	全てのコン パーネント 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)。	5
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						
\.2.2.2						冗長化(コンポーネント)	非冗長構 成	ンポーネン	全てのコン パーネント 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)。	:
.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)	成	長化	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。 【レベル1】	5
						ポーネント)	成	ンポーネントのみ冗 長化	/ ポーネント を冗長化					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。	5
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。 ポ。		回線の冗長化	冗長化しない	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。	
A.2.4.3						セグメント分割	分割しない	サブシスラ ム単位で 分割	一用途に応 じて分割					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。 【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。	-
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	全ての機 器を冗長 化					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。 【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。	
									A = 0 - 1					【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。	5
A.2.5.2							成	ンポーネン トのみ冗 長化	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。	16
x.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		オンライン バックアッ プ	バックアッ プ+オンラ インバック				【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。	:
										アップ				【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。	

(付録)

					重重	i ジトリクス			レベル	ル			運用コ		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
	大項目	中項目	小項目	小項目説明	複 項 目	[(指標) 	0	1	2	3	4	5	ー ストへ の影 響	1用	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.2.6.2						データ復旧箪 囲]		ステム の全 ータを復					【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。						
					0									【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	エラー検は出無しは	エラー検 エラ 出のみ 出る 行	[4]	呆障				【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。						
									出	エラー検 出&訂正)				【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		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	いが	限定され 同- た構成で 成で システムを テム 再構築 構刻	でシス た ムを再 D	根定され c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。						
														「構成は旨くなど」を思いする。 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。						
A.3.2.1				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		保管場所分 散度	外部保管 1 しない			カ所 遠隔地)										
A.3.2.2				の要求。		保管方法	る保管 F 	司一サイト DR 内の別スト への レージへ モー のバック クア アップ	のリ ートバッ											
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。	五	災害対策範 囲	対策を実 特施しない 第	特定の対 想象 策を実施 全で	ての対 を実施					【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。						
								9 %						【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						
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		復旧用製 復日 品は使用 品口 しない手 復日 作業の復	による 品 旧 ア シ	复旧用製品+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。						
					0				6	の接口				【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					0	代替業務運 用の範囲	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	一部の業 全部 務につい 務I て代替業 て作 務運用が 務選 必要 必要	につい 代替業 運用が					【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。						
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	実施しながい。またはが単純な障がまの範囲が	業務を継 業務 続できる とな 障害の範 のこ の	務停止 業 る障害 と うち一部 の 節囲 範	業務停止 ☆なる障害 の全ての 節囲				【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	業務停止となる障害が発生しても、 復旧方法が自明であり、確認の必 要がない場合。	害のうち	業務停止となる障害に対しての対策を確認する必要があるが、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	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 確認が必要な場合。
					0					-0123						[-] 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	囲	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	77-51-2	[-] 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
																ておく必要がある場合		[+] 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		
B.1.1.1	性能•拡張 性	業務処理量	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	.	ユーザ数		上限が決 不特 まっている 数0 ザカ						【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。		部門内利用などでユーザが特定できる場合を想定。			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。
				でなく、前提となる時間帯や季節の特性なども考慮する。										【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。		[+] ユーザを特定できない場合		[-] 特定のユーザのみ使用すること を合意できた場合		[-] 一定の上限値を設定することが 可能な場合
B.1.1.2					0	同時アクセス 数)	特定利用 『 者の限ら - れたアクセ』 スのみ	司時アク 不特 セスの上 数の 限が決 セス まっている	特定多 のアク 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。	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。	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	データ量 ⁻ が明確で (主要な データ量 のみが明						【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。	データ量 が明確で	要件定義時には明確にしておく必要がある。	データ量 が明確で	要件定義時には明確にしておく必要がある。	データ量 が明確で	要件定義時には明確にしておく必要がある。
							ある 4	確である						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。	ある	[+] 全部のデータ量が把握できてしない場合	、 ある	[+] 全部のデータ量が把握できてい ない場合	ある	[+] 全部のデータ量が把握できてい ない場合

				重	重	7		レ	ベル		運用		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	影響が極めて大きいシステム
項番	大項目	中項目 小項目	小項目説明	複項目	 要 メトリク! 項 (指標) 目	0	1	2	3	4	スト/ の影		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.1.1.4				(オンライン クエスト件		主な処理のリクエスト件数のみが明確である	ζ.				【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。	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	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	リクエスト 件数が明	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 数 〇	件数が決	z 主な処理 ! の処理件 ! 数が決 る 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】	毎に処理 件数が決	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	毎に処理 件数が決 まってい	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	毎に処理 件数が決	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
B.1.1.6					安 攻 1 4 4 4 5	Kh ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' ' '		*** 3女 +&				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。						
B.1.1.0					未伤饭肥		では、 業務機能 一覧が作 成されて	一覧はあ	宦			【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。	点	ユーザ数5大率	自 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		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	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
B.1.2.2					同時アクセ数増大率	2ス 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。		合 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。	1 1.2倍	合 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。
					0									ラスといるかを確認する。 [+] 利用者の増加が見込まれる場合		ラス C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		[-] 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
B.1.2.3					 データ量堆 率	<u></u> 曾大 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。		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。		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。
					0									[+] 段階的稼働や、マスター蓄積システムの場合		[-] 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		[-] 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 クエスト件 増大率		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。	0 1倍	システムの制約となるリクエスト数 の見通しを確認する。	1 1.2倍	システムの制約となるリクエスト数 の見通しを確認する。	1 1.2倍	システムの制約となるリクエスト数の見通しを確認する。
B.1.2.5					バッチ処理 数増大率	里件 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】	0 1倍	システムの制約となる処理件数を確認する。		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.1.2.6					業務機能	数 1倍	1.2倍	1.5倍	2倍	3倍	10倍以上	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。 【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。						
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。	5	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。 【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。		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		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	有期	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
B.1.3.2	_				対象範囲	で参照で	ノ アーカイブ まで含め	ĵ				【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	,			[+] ディスク容量に余裕がある場合		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 オンラインレポンス	ス オンラインシステム利用時に要求されるレステンス。 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、過	<u>:</u> す す	通常時レスンス順守率	きる範囲 スポ 順守率を 定めない	る - 60%	80%	90%	95%	99%以上	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。 【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。	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。		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。	5 99%以上	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
B.2.1.2	_		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)	ス	ピーク時レ ポンス III デ	·ス 順守率を F率 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。		[+] 性能低下が、システムの評価 低下につながる場合 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	2 80%	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 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		合。または代替手段がある場合 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
						, — LC0//66'						具体的な目標値や利米値がある場合、各処理の順寸率を放足する。 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。		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		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		標値を達成できれば良いと想定。 [一] 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

					重重	メトリクス			レ	ベル			運用=		社会的	影響が殆ど無いシステム	社会的	り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
項番	大項目	中項目 小項目	3	小項目説明	後 安 項 項 目 目	(指標)	0	1	2	3	4	5	の影響	備考 	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.2.1.3						縮退時レスポ レス順守率	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 ス(ターンフ ンドタイム)	アラウ ス) 3 (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	0	通常時レスポ レス順守度合 ハ	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。	いを定め	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。	余裕が確	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。	余裕が確 時の 保できる 不正 あれ	対象とする処理の中で、通常 バッチ処理を実行し、結果が の場合、再実行できる余裕が ば良いと想定。
			H 1	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		° 4n+1 =		T O O O	T									[-] 再実行をしない場合または代替 手段がある場合	手段	再実行をしない場合または代替 がある場合
B.2.2.2				決めておくことが望ましい。 (例:日次処理/月次処理/年次処理など)	0	ピーク時レス ポンス順守度 合い	順寸度合いを定めない	所定の時間内に収まる	再美行の 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。	いを定め	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。	余裕が確	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。	余裕が確 時の保できる 不正 あれ ピー はサ	対象とする処理の中で、ピーク バッチ処理を実行し、結果が の場合、再実行できる余裕が ば良いと想定。 ク時に余裕が無くなる場合に 一バ増設や処理の分割などを する必要がある。
B.2.2.3						宿退時レスポ レス順守度合		所定の時間内に収						【レベル1】 所定の時間には再実行は含まない。				[-] 再実行をしない場合または代替 手段がある場合		再実行をしない場合または代替 がある場合
B.2.3.1		ナニハ	7 -	オンラインシステム利用時に要求されるスルー	L	通常時処理		まる 1.2倍	保できる	2倍	3倍	10倍以上		【レベル】						
		オンライン: ループット	- 3 1	インフィ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	É		(余裕無し)) 1.21日	1.51급	21 a	্ব্যান্ন	10倍以上		についた。 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			五年	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/		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				がが、アーダエントリ件数/時间、貝のパり回数/ 分、TPSなど)	*	縮退時処理 余裕率	縮退をしな い	1/2の処理	通常時と 目 同様に処 理が出来						-					
B.2.4.1		バッチスル 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	É		(余裕無し)	1.2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				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		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			<i>t</i> U	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	9	縮退時処理 余裕率	縮退をしない	1/2の処理	通常時と 理 同様に処 理が出来 る											
B.2.5.1		帳票印刷館	能力 巾	送信処理など) 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		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			ì	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。		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	1/2の印刷	通常時と 間 同様に印 刷が出来 る											
B.3.1.1		リソース拡 CPU拡張性 張性	C	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	C	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。	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。	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。	1 50%以上 業務 80%未満 せて	活量の増加に備え、余裕を持た いる状態を想定。
			7	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。	0									【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。		[+] 近い将来利用者が増える予定 がある場合		[-] 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	ことで [+] i	生能・拡張性より低コストである を優先する場合 近い将来利用者が増える予定 る場合
				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。										【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。						
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	張 8倍以上 拡張がす 能	の I	0	【レベル】 CPU搭載余裕がある機器は無い機器より高コストである。 【運用コストへの影響】		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。		3年後のシステム拡張に備え、 増設を可能にしたと想定。
														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。						
B.3.2.1		メモリ拡張	,	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	,	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		システムが過剰設備となっていな いという想定。		業務量の増加に備え、余裕を持た せている状態を想定。	1 50%以上 業務 80%未満 せて	活量の増加に備え、余裕を持たいる状態を想定。
			石 カ オ 言	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									0	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】		[+] 近い将来利用者が増える予定 がある場合		[-] 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	ことで [+] i	生能・拡張性より低コストである を優先する場合 近い将来利用者が増える予定 る場合
Dog of				ソース専有の有無」で確認する。		▞ ▗▄▗▗▗ ▘ ▗▗ ▗ ▗	4 / \$	1 5 5 5 12		1 1 5 5 1 1 -	TE OF THE			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。		如明中四ウのゼロッケリ ・ー・・-	1 2 - 1 to - 1	0.054017-147-147-147-147-147-147-147-147-147-1	1 1 1 1 1 1 1	0年後の2 ユニノ は12.1 - "" -
B.3.2.2						メモリ拡張性	は協・技術の表示である。	1.5倍の拡 は 張が可能	X 2倍の拡張 が可能	4倍の拡張 が可能	張 8倍以上 拡張がす 能		0	【レベル】 メモリ搭載余裕がある機器は無い機器より高コストである。 【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。		部門内限定の利用であり、メモリの 拡張が不要な場合		、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。		3年後のシステム拡張に備え、 リ増設を可能にしたと想定。

					重重	メトリクス		l	ノベル	_	_		用コ	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	社会的景	ジ響が極めて大きいシステム
項番 大项	項目 中	中項目	小項目	小項目説明	重複項目	(指標)	0	1 2	3	4	5	σ,	トへ)影 響	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.3.3.1			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	·	ディスク利用 率	80%以上 58	0%以上 20%以上 0%未満 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。						
				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								,	「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。						
B.3.3.2				を確認するための項目。	ラ 性	ディスク拡張 生	1倍 1 (拡張要求 引 なし)	.5倍の拡 2倍の拡 長が可能 が可能	張 4倍の拡張 が可能 	₹ 8倍以上の 拡張が可 能			【レベル】 ディスク搭載余裕がある機器は無い機器より高コストである。						
												(〇 【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。						
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		ネットワ <i>ー</i> ク 機器設置範 囲		7ロア内の 同一拠, AN (ビル)内 LAN	気 社内複数 の 拠点間の 接続 (LAN.	社外拠点 との接続									
				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。					WAN)										
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		スケールアッ プ	アップを行し	-部の 複数の ナーバの サーバる みを対象 対象	Ē				【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タ						
				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									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 ケールアップする場合を想定。	Z					
				し、サーバ台数を増やすことで処理能力の増 強を行う。									【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					7	スケールアウ、	アウトを行り	-部の 複数の ナーバの サーバる みを対象 対象	Ē				【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】						
B.4.1.1	性能			ネットワークのサービス品質を保証する機能		帯域保証の	無し	プロトコル 各サーバ	・ アプリケー	- [_	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。	_					
	証		の有無	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 <mark>ある</mark> 。		设定	耳	単位で設 毎に設定	ミーションのエーンドツーエーンドで検ー証・保証ー										
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	与り(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。		則定頻度	測定しながい	構築当初 運用中、 に測定 必要時/ 測定可能	運用中、 定常的に は 測定										
B.4.2.2					Ãí	雀認範囲	い	-部の機 全ての根 能につい 能につい て、目標値 て、目標 で満たして を満たし	· E値										
							L 研	いることを いること 確認 確認	を										
B.4.3.1			スパイク負荷対応	耐 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		・ランザクショ ヶ保護	ション保護 t は不要で 数	同時トラン 同時トラ ボクション ザクショ 数の制限 数の制限 機能にた え、Sorr 動作	ン Sorry動作 艮 を行うサー I バの設置	-									
C.1.1.1 運用・ 性	·保守 通常	常運用	運用時間	装し対策する場合が多い。 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、	常	運用時間(通 常)	規定無し 気(9時~17 停止	り 1時間程度 の停止有 1 り	と 若干の停止有り (9時~翌	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 停止	ト 夜間に実施する業務はなく、システムを停止可能。	4 若干の停 248 止有り が、 (9時~翌 せん	極力システムの稼働は継続さ		システムを停止できる時間帯が存 在しない。
				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。				寺) (9時~2 時)	(9時~翌 朝8時)				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。	(9時~2 時)	│ [-] 運用時間をもっと限って業務を 稼働させる場合 [+] 24時間無停止やリブート処理等 の短時間の停止のみを考える場合	朝8時55 分) [-]	る。 夜間のアクセスは認めないな 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		[-] 1日のスケジュールで定期的に 運用を停止する時間帯が存在する 場合
					0 0								【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		の及所的の行业のからでもんの物に		24時间無け近く注用する物は		
													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るる時間帯を指す。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	5					
C.1.1.2					道	運用時間(特 定日)		9時~17 停止	り 1時間程度 の停止有	止有り	停止	#	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。 【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		通常と異なる運用時間となる特定 日は存在しない。	停止め、	まはバックアップ運用のみのた 夜間は停止する。		システムを停止できる時間帯が存在しない。
							i i i i i i i i i i i i i i i i i i i	寺) (9時~2 時)	1 (9時~翌 朝8時)	(9時~翌 朝8時55 分)			目となっている。 【メトリクス】		 [+] 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	(9時~21 時) [-] バ ゾ	週末運用するバックアップや ッチ処理などが存在せず、土休		[-] 定期的に運用を停止する日が 存在する場合
					00								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。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	ĕ	る特定日が存在する場合	[+]	は運用を停止する場合 休日出勤する社員の業務に必 なため、土休日も運用する場合		
													合すること。						

				重重重複響	重 メトリクス			レ	ベル			軍用コ ストへ		社会的	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
項番	大項目	中項目 小項目	小項目説明	項項項目	ま 頁 (指標) 目	0	1	2	3	4		の影響	備考	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.1.2.1		バックアッ	プレステムが利用するデータのバックアップに する項目。	関 O	データ復旧筆 囲	復旧不要		内の全	Ī				【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。						
							±0.0	LI +0 - °					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				C	外部データ <i>0</i> 利用可否	の復旧に	一部の データ復 旧に利用 できる	タは利用					【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。) 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	y 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、そちらからデータを持ってきてシステムを復旧できるような場合	タは利用 アップできない いこ [-] が なが 障害	ータを復旧するためのバックプ方式を検討しなければならなとを想定。 外部に同じデータを持つシステ済在するため、本システムにが発生した際には、そちらから少を持ってきてシステムを復旧るような場合
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	ラーからの	データの 長期保存 (アーカイ				【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ークアップも考慮すること。			ラーから	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。	3 データの 内部	る 統制対応の要件に基づき、 タの履歴を保存する必要があ
				C			正		ブ)				【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。	; 	[-] 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	Ē	[-] 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	ブ) [-] / の回 る場	バックアップはデータ損失から 復に対する用途にのみ使用す 合
C.1.2.4				C	バックアップ 自動化の範囲	全ステップ を手動で 行う	プ <mark>ー部の</mark> ス テップを手 動で行う	を自動で	全ステップ を自動で 行う			0	【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 ・バックアップ大メディアの選択 (テープ交換) ・ファイル転送 などといった作業ステップが存在する。 別地保管を媒体搬送で行う場合の、テープ交換はここには含まない。 【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。	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。 [-] スクリプトを作成せず管理者が全てのステップを手動で実行する場合 [+] バックアップに関する管理者のオペレーションを削減したい場合	テップを	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ブ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	プを自動 ン(ス で行う 理、 フト・ を想	クアップに関するオペレーショスケジュール管理、メディア管ジョブ実行等)に関して、管理ソウェアを導入して自動で行うこと定。 管理者が手動でバックアップをする場合
C.1.2.5				C	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 更意のな イミング	月次で取得	週次で取得	日次で取得	司期バック アップ		なるため、その方達用コヘドは減少すると考えられる。	構成の変 更時な 受いを の タイミン グ	バックアップから復旧する必要のあるマスターデータ等は、運用中ほとんど更新されることがないため、定期的にではなく、マスターデータ更新時にバックアップを取得することを想定。 [+] バックアップから復旧する必要のあるデータがトランザクショナルなデータで運用中随時更新されるようなものである場合	: 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	クアップ 容を障害 DRサ	の要件を満たすため、更新内 バックアップサイトへ転送し、 発生時にすぐに運用が可能な サイトを構成することを想定。 章害発生時にバックアップから カバリ作業のため運用の停止 されるような場合
C.1.2.6				C	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 ź 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	-	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	有限 され [-] f シス [+] f	ているような場合を想定。 呆存先容量の制限で10年分を テム上に保持できない場合 呆存先容量に制限がなく、永続 データを保管しなければならな
C.1.2.7				0	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。						
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。	含した	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(ト) 報を行う	リソース監視を行う	パフォーマンス監視を行う	0	【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。	対 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のみを通知できればよい。 [-] ハードウェアやプロセスの死活状態のみが判断できれば良いような場合 [+] 障害対応時間の短縮のため、管理者が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	だ 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	監視を行 う う 「一」『の 「十」間 シス	使用率やスワップの発生状況 対して閾値を設定し、サービス ル低下の予兆を監視して、シス の拡張計画や運用スケジュー 検討を行うことを想定。 章害の発生を検知して管理者 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の スループットなど、より厳密に テムのサービスレベルを評価 いような場合

					重重	メトリクマ			レベ	ドル			運用コ	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 -
項番 力	大項目	中項目	小項目	小項目説明	項項目	メトリクス (指標)	0	1	2	3	4	5	ストへ の影 響	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.1.3.2					0		監視を行 わない	不定期監 (視(手動監 (E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	(分間隔) 監とこ。 [-: の て況:	害を検知するまでの時間がかってしまうが、システムに対する 視情報収集のコストを低くするこを優先し、分間隔での監視とする とを想定。 〕障害の検知はアプリケーション 機能で実装し、システム基盤とし の監視としては定期的な運用状 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 いような場合	ム監視	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.1.3.3) 	レステムレベ レの監視	- 監視を行 わない	一部監視 全を行う を	全て監視 そ行う				【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】						
C.1.3.4						for Late &	56-40-4-4-	±77.555.4B ∧	~ FF 4P				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。						
G.1.3.4							監視を行 わない	一部監視(全を行う)を	ご(監視)				【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					ラレれ	データベース vベルの監 見	. 監視を行 わない	一部監視 全を行う を	全て監視 −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					7	ストレージレ ドルの監視	監視を行わない	一部監視全を行うを	≧て監視 ÷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					+; <u> </u>	ナーバ(ノー ゛)レベルの 監視	監視を行 わない	一部監視全を行うを	全て監視 - 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。						
C.1.3.8						端末/ネット フーク機器レ ドルの監視	監視を行わない	一部監視 全を行う を	≧て監視 ÷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					/	ペットワーク・ ペケットレベ レの監視	監視を行 わない	一部監視全を行うを	全て監視 そ行う				【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。	5	寺刻同期設 Eの範囲	を行わな	サーバ機 サ 器のみ時 よ 刻同期を ア 行う に	くびクライ アント機器 こついて	ク機器も 含めシス テム全体	全体を外部の標準時間と同		【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。						
		/B 点次	<u> </u>	上协作业以及和社工				時 を	特刻同期 そ行う -	で時刻同期を行う	期する		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。	<u> </u>	古並の人立 ピナレノピー サー・・・	4 1=1== N= 1 1=-	吐用毎点ル~の字四パンで、「	o 1=1- 	シ. フ. ニ / ナ/左 / マンフホロロル パン・ コ
G.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。	ま	有無	有り(運用 スケジュー ルの変更	計画停止 有り(運用 - スケジュー ルの変更 不可)					【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。	有り(運 用スケ ジュール の変更		有り(運 い 用スケ 画 ジュール の変更不 [-] 可) 前	時間無停止での運用は必要な。停止可能な時間が存在し、計的な停止は可能。 」運用スケジュールとしては停止能な時間帯は存在しないが、事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	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

社会的影響が限定されるシステム

選択時の条件

[-] 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

選択レベル

社会的影響が極めて大きいシステム

選択時の条件

[-] 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

選択レベル

1 一部の保 業務機能の起動・停止など定期的 さ 全ての保 業務機能の起動・停止やスケ 守作業を に行う処理は自動化するが、ログ 自動で実 の削除など非定期に実行する処理 行する は管理者が手動で実施することを 行する 定 な においま また は でまた に できた は でまた に できた は できた に できた に

TZ.	+ -= -	++= -	,i. += ==		重重	メトリクス			レ <i>/</i>	ベル		運用:		社会的	内影響が殆ど無いシステム T	
番	大項目	中項目	小項目	小項目説明	重複項目	は(指標)	0	1	2	3	4	5	影 循一	選択レベル	選択時の条件	選
						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	0	【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。			
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。	C	保守作業自 動化の範囲	保守作業は全て手動で実施する	守作業を	全ての保守作業を自動でる			0	【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、点検作業やパッラ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、さまさ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。	· 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	
2						サーバソフトウェア更新作業の自動化	の更新ファイル配布	アの更新ファ	の更新ファ イル配布 機能を実	の イ機 機 表 更 和 能 し 、 新 自 行 と 更 を 配 を 配 を 配 を の の り の り り り り り り り り り り り り り り り		0	【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。			
; ;						端末ソフト ウェア更新作 業の自動化	端末への更新できます。現代では、東新ファイル配布機能を実施しない	ル配布機 能を実装 し、手動に て配布と 更新処理	ル配布機 能を実動で し、布した のち、更新	ル配を まれる に、 新動 を は、 が が が が が が が が が が が が が が が が が が		0	【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。			
			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	要求に応じてベンタが受動的にパッチリ	定期的に ユーザへ パッチリ リース情 報を提供	アルタイム に(パッチ リリースと 同時に)							
2						パッチ適用方針			パッチを適	i			【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)。	-		
.3						パッチ適用タ イミング	パッチを過 用しない	意 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)。			
4						パッチ検証の 実施有無	パッチ検 証を実施 しない	チのみ	障害パッ チとセキュ リティパッ チのパッチ でパッ実施 する							
.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	ハードウェ アにおい	アにおい て活性保				【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。			
2						ソフトウェア 活性保守の 範囲	活性保守 を行わな い	において	トウェアに おいて活				【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。			
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		半年に1回	月1回	週1回	毎日		1		
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	予防保守を実施したい	の範囲で	とは別に)一定間隔	ムに予兆 検出を行 い、対応を 行う						

						重重複要メトリクス項項(指標)	L	ベル			運用コストへ	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
項番	大項目		中項目	小項目	小項目説明	頃頃 (指標)	0 1 2	3	4	5	の影	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.3.1.1		障害	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 復旧用製 品は使用 品による しない手 復旧 作業の復	品+業務 アプリケー	-		【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。	Г					
							旧	ションによ る復旧			【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。						
						0					【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、どるまで自動化するか(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。	=					
C.3.1.2						代替業務運用の範囲	務につい 務につい て代替業 て代替業 務運用が 務運用が	·			【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。	:					
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。	動化の範囲	障害復旧 一部の障 全ての障 作業は全 害復旧作 害復旧作 て手動で 業を自動 業を自動 実施する 化する 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 うようなケースを指す。	ਰਿ ਹਿ					
											○ 【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。 め運用コストは減少する。	o te					
C.3.3.1				システム異常材 知時の対応	策 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。	間	ベンダの 営業時間 内(例:9時 時間帯 ~17時)で (例:18時 対応を行う 対応を行う 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。						
C.3.3.2						駆けつけ到着時間	保守員の 駆けつけ 無し 無し 数日中 第2 第2 第4 第5 第4 6 第4 第4 第4 第4 第4 第4 第4 第4 第4 第4 第4 第4 第4	保守員到常 検知からの 翌営業 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の駆け SE到着が SE到着か 内側 大田 大田 大田 大田 大田 大田 大田 大	が SE到着が 異常検知 からユー ザの翌営 業開始時 まで	異常検知		【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 保守契約 保守契約 に基づき、保守支がき、保守するが、保守するが規 はずが規 定年数の 間保守部 品を確保する は は かって 関係 は ない は は が は ない は は が は は ない は は は ない は は は は				【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 一部、予 全部、予 し 備機有り 備機有り										
C.4.1.1		運用	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。	の設置有無	システム の開発環 境を設置 しない運用環境 と同一の 開発環境 を設置す を設置する る	ŧ I			【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。本稿 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。	番 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	の一部に 限定した [-]	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 する場合	と同一の 開発環境 を設置す	本番環境と同等の開発用環境を置することを想定。 [-] 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 用意する場合
C.4.2.1			1172	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。	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 用する専用の試験環 験用環境 を設置す る	<u> </u>			【メトリクス】	番 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	の開発用 環境と併 [-] [*] 用する [+]	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 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 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f レベル	# 運用のためのマニュアルの準備のレベル。	備レベル	各製品標 準のマ の通常運 の通常運 ニュアルを 用のマ 用と保守 利用する ニュアルを 運用のマ 提供する ニュアル・提供する	☑ システム 運用ルー ルに基づく			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。 【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。	準のマ ニュアル を利用す	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。	の通常運 を実 用と保守 業引 運用のマ ルも ニュアル	は時にはユーザ側にて保守対応施することも想定し、リカバリ作・順などを示した保守マニュア作成する。 保守作業は全てベンダに依頼	システム 運用ルー ルに基づ くカスタマ	ユーザの自営センターの運用ルルにのっとったマニュアルの作成要望。 [-] ベンダの用意する一般的な選用マニュアルで良いような場合
								ニュアルを提供する			〇 【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。		[+] ベンダよりマニュアルの提供を 受ける必要がある場合	る する レー ニュ [+] 味し	たが作業は宝でヘンダに依頼ため、通常運用に必要なオペションのみを説明した運用マアルのみ作成する場合ユーザ独自の運用ルールを加た特別な運用マニュアルを作る場合	イスされ たマニュ アルを提 供する	ハ」、一ユノ ル C 区 いみ J/d 場 目

			重重		ν	ベル		運用		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
項番	大項目	中項目 小項目 小項目説明	Tell	0	1 2	3	4 5	ー	影	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	視を行わ ない	構内LAN 遠隔地で を介してリ リモート監 モート監視 視を行う を行う	Ē		C	【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	機器数が少ないため、リモートでの 集中監視を行わない。 [+] 機器数が少なくとも、別途監視 サーバを用意してリモート監視を行 う場合	を介して リモート 監視を行 う	センターに配置されるサーバ機器のみリモート監視を行い、各支店に配置されるクライアント機器類は監視を行わない。 [-] サーバ機器についてもコンソールでの直接監視を行う場合 [+] 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 システムを構成する全ての機器 を監視センターからリモートで 監視を行う 監視を行う ここ リモートで監視を行うのはも ターに配置されているサーバ機 類のみとし、各支店に配置されるクライアント機器類はコンソーにて直接監視してもらうようなな
C.4.4.2			リモート操作の範囲	作を行わ	定型処理 のみり モート操作 を行う を行う	ŧ		C	【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。		メンテナンス操作は、全てマシンローカルの環境で実施する。 [+] 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	のみリ モート操 作を行う	集中監視を行っているリモート監視端末から、対象機器のメンテナンス操作を実施することを想定する。セキュリティの観点から、あらかじめ実行できる操作を限定する。 [-] 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 運用部門とシステム設置場所だることを想定し、 にを行う 機器の操作を基本的に全てリートで実施できるようにする。 [-] 特定の操作のみの実行がればよいような場合
C.4.5.1		外部システム接 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 デムと接 続しない	社内の外 社外の外 部システムと接続 する 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。		部門内システムであり、連携する他システムが存在しない。 [+] 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	部システ ムと接続 する	企業内基幹系システムとして、受発注と在庫管理などのように連携する社内の他システムが存在することを想定。 [-] データのやり取りを行う多システムが存在しない場合 [+] 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 社会基盤のシステムとして、様部システムと接続 企業システムと連携して処理をシステムを想定。 「一」システムと連携する外部のテムが存在しない場合
C.4.5.2			監視システム の有無	ム 監視シス テムは存 在しない	既存監視新規監視システムシステムに接続すに接続す				【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	乗 システム	る る 既存ジョブ 新規ジョブ 管理シス テムに接 テムに接 続する 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		サポート体保守契約(ハードウェアの範囲。制	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 ポート契約 ウェア)に 対しての 部対象外 み保守契 約を行う	ンダのサ カポート契約 を行う(シ		C	【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。	自社製品 (ハード ウェア)に 対しての	システムを構成する個々のハードウェア製品を調達し、SIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	ンダのサ ポート契 約を行う (一部対 象外を許 容)	既存の機器を流用したシステム構築を想定。既存の機器に対するサポートは、別ベンダが実施する。 [-] 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 おを一本化し、管理者の負荷を軟がを行う (システム を構成する全製品を対象) トラマン を対象) システムの構築を行う場 など、一部の製品に関して問いたシステムの構築を行う場 など、一部の製品に関して問いたシステムの構築を行う場 など、一部の製品に関して問いた。
C.5.2.1		保守契約(ソフトウェアの範囲。トウェア)	保守契約(ソ フトウェア)の 範囲) を行わな い	ベンダの マルチベ 自社製品 (ソフトウェ ポート契約 ア)に対し を行う(一てのみ保 守契約を 行う	ンダのサ		C	【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。	自社製品 (ソフト ウェア)に 対しての	システムを構成する個々のソフトウェア製品を調達し、SIはユーザが実施することを想定。 [+] SIerを立てて、システム全体を調達するような場合	ンダのサ ポート契 約を行う (一部対 象外を許 容)	既存のソフトウェアライセンスを流用したシステム構築を想定。既存のソフトウェアに対するサポートは、別ベンダが実施する。 [-] 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 かることを想定。
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	3年以内には組織変更が発生し、システムの更新が必要となることを想定。 [+] 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		間に合わせてシステムのライフサイクルを7年と決定したと想定。 [-] 導入するソフトウェアやハードウェアのサポート期間がもっと短い場合 [+] 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	3 10年以上 システムで実施する業務は今代年間は継続することになるため、ステムのライフサイクルをそれわせることを想定。 [-] 導入するソフトウェアやハーウェアのサポート期間が短いたそれにあわせてライフサイクルを定める場合
C.5.4.1	1	メンテナンス作 メンテナンス作業に対するユーザ/ベンダの役業役割分担 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					I	1	<u> </u>	イクルを合わせる場合	<u> </u>
C.5.5.1	_	一次対応役割 一次対応のユーザ/ベンダの役割分担、一次 分担 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 全てベン ザが実施 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		ベンダの 夜間のみ 定時時間 非対応(9 内(9~17 ~21時) 時)	に1時間程	応							

				重重	,,			レ	ベル			運用コ		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
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)	0	1	2	3	4	_ (ストへ の影	備考	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.5.6.3					ベンダ側対応 者の要求ス	指定無し	有識者の指導を受けて機器	システム の構成を	システム の運用や	システム の開発や									
					キルレベル		Iの操作を	クの収集・ 確認が実	手順に習 熟し、ハー	わり、業務 要件や									
							న		ソフトウェ アのメンテ	ユーザの 事情にも 通じている	,								
									ナンス作 業を実施 できる										
C.5.6.4	1				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						
C.5.7.1	+	<u> </u>	算入サポート 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	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上		(の待機方法について確認する。						
			O.Wileio		入サポート期間														
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									
C.5.8.1	1		オペレーション オペレーション訓練実施に関する項目。 訓練		オペレーション訓練実施	実施しな い	全てユー ザが実施	ー部ユー ザが実施	全 て べ が 実施										
C.5.8.2	_				の役割分担 オペレーショ	実施しな	通常運用	通常運用	通常運				【レベル】						
					ン訓練範囲	い	実施	に加えて 保守運用 の訓練を 実施	運用に加				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。						
									復旧作業										
0.5.0.0					→ •°1 • • •	中长一大	S.7 = 1	占如眼 炒	訓練を実 施										
C.5.8.3					オペレーショ ン訓練実施 頻度	天他しな	システム 立ち上げ 時のみ	正期開惟											
C.5.9.1		5	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。						
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	障害およ び運用状										
								報告を行う	加えて、改善提案を										
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	内部統制対応につ	既存の社 内規定に	新規に規定を制定	117				【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	0 内部統制 対応につ	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。	1 既存の社 社内 内規定に 実施	R規定に従い、内部統制対応を Rする。	1 既存の社 法令(内規定に 部統領	こて定められているとおり、内 制対応を実施する。
					無 無	いて規定 しない	従って、内 部統制対 応を実施	し、内部統 制対応を					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。	いて規定 しない	[+] 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	従って、 内部統制 [-]	内部統制実施の対象システム ないため、対応を実施しない場	従って、 内部統制 [-] 順 対応を実 統制規	 守すべき法令や社内の内部 現定等が存在しない場合
							する								する場合	施する 合 [+] シス	既存の規定は存在しないが、本 、テムを構築するに際して、新た	施する [+] 既 シスラ	存の規定は存在しないが、本 ・ムを構築するに際して、新た 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		サービスデス	サービス	既存の	新規に					【メトリクス】	0 サービス	ユーザ/ベンダ間のやり取りに関し	1 既存の マル	記定を策定するような場合 ・チベンダのサポート契約を締		ンステム専用のサービスデス
			提供するかどうかに関する項目。		クの設置有無	デスクの 設置につ いて規定	サービス デスクを利 用する	サービス デスクを設 置する					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。	設置について規定	てサービスデスク機能を設けず、個別対応にすることを想定 	デスクを ビス 利用する	「るベンダとの間に既存のサー デスクが存在することを想定	デスクを 定 設置する	じをベンダが開設することを想
				0		しない								しない	[+] サービスデスクを設置する場合	 	サービスデスクを設置しない場初めて取引を行うベンダで、既		存のサービスデスク機能を利 るような場合
								*C+0 /)サービスデスクが存在しない な場合		
C.6.3.1		Į	インシデント管 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	ト管理について規定	ンシデント 管理のプ	ンシデント 管理のプ					【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		問題答理へ	世野管理	従う	ロセスを規定する					「メトリクフ 】						
U.6.4.1			問題管理 インシテ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	について	題管理の プロセスに	題管理の					【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		構成管理の	構成等理							【メトリクス】						
0.0.3.1		[†]	構成管理 バードウェアやウンドウェアなどのT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。		実施有無	について	成管理の プロセスに	成管理の					(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		変更管理の	変更管理	既存の変						唯 総 後 に 具体 化 し く 唯 総 す る 。 【メトリクス】						
3.0.0.1			のプロセスを実施するかどうかに関する項目。		実施有無	について	更管理の プロセスに	更管理の					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	_		J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		リリース管理	リリース管	既存のリ	新規にリ					【メトリクス】						
3.3.7.1			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。		の実施有無	理につい	リース管 理のプロ セスに従う	リース管 理のプロ				,	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。						
							pc y	定する											

					重重	メトリクス			レ	ベル			運用:		社会	ま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	会的影響が極めて大きいシステム
項番	大項目	中項目	小項目	小項目説明	復 安 項 項 目 目	(指標)	0	1	2	3	4	5	の影響	備考	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 其	ンステム移行 明間	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	システムを短期間で構築する必要がある。 [+] 中長期間で進める場合	4 2年未満	年度を跨いで移行を進める必要がある。 [-] 期間短縮の場合 [+] さらに長期期間が必要な場合	5 2年以	上 移行の計画から稼働まで安全性 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						ノステム停止 可能日時	制約無し (必要な期 間の停止 が可能)	5日以上		(計画停山	止ない時間	か 移行のた 引 めのシス な 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】 レベルの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。	1 5日以上	業務への影響が少なく数日以上はシステム停止可能。[-] さらに停止を多くする場合[+] 停止を少なくする場合		業務が比較的少ない時間帯にシステム停止が可能。 [-] 停止を増やす場合		のた システム停止時間は最短にする。 シス 要がある。 亨止 [-] 停止時間を確保する場合
D.1.1.3					立章	位行稼働の 頁無	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も 十分確保できるため並行稼働の必 要性は低い。 [+] 移行のためのシステム停止期 間が確保できず、並行稼働する場 合	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		移行のためのシステム停止不可でため、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の程度。		拠点展開ス 「 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 満	k 20段階以 上	以 ·	【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 のため 規定無	1 点 システムが単一で展開を規定する 必要がない。 上 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 段階的展開が必要である。 [-] 一斉展開する場合 [+] 段階数を増やす必要がある場合
D.2.1.2						テップ数	単一業務のため規定無し	斉切り替	4段階未満	6段階未満	満 10段階 # 満	10段階以 上	N	【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 のため 規定無	タ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 満	法 段階的展開が必要である。 [-] 一斉展開する場合 [+] 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。		设備・機器の 多行内容		設備・機器 のハード ウェアを入 れ替える		設備・機器 のシステ ム全部を 入れ替え	器 設備・機のシステム全部を	器 - - - :		【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: 無し	設備機器を新設する必要がある。[+] 既存設備機器が存在する場合	設備・機器のシス	┃ [-] 業務アプリケーション更改が無	設備・ 器の/ ドウェ OS、ミ ルウュ	
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)。	0	多行データ量	無し								1 1TB未清			1PB(ペタバイト)未満のデータを移行する必要がある。 -] 1TB未満の場合 +] 1PB以上の場合		以上 1PB(ペタバイト)以上のデータを 行する必要がある。 [-] 1PB未満の場合
D.4.1.2					和 O	多行デ ー タ形 t	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。	1 移行先。 形式が 一	と データ形式を現状のままで使用す 司 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	形式加	先と データの継続性や他システムとの が同 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
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。	科	多行媒体量	移行対象 無し	10本未満 (1TB未 満)	満	1000本以 上 (1PB以	l.							ļ	I	
D.4.2.2					为	多行媒体種 頁数	無し				 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)。	科の		無し 移行ツー ル不要 またた移行 ツールで	変換ルー ル数が 10未満 の移行 ツールの	変換ルー ル数が 50未満 の移行 ツールの	変換ルー ル数が 100未満 の移行 ツールの	・ 変換ルー ル数が 100以上 の移行 ツールの									
D.5.1.1		移行計画	移行作業分担	移行作業の作業分担。	+	多行のユー ザ/ベンダ作 	全てユー ザ	複雑度 ユーザと ベンダと共 同で実施	全てベン		複雑度 			【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)。	J B	ハーサル範 王	リハーサ ル無し	主要な正 常ケース のみ	常ケース	ス+移行 前の状態 に切り戻 す異常	正常ケース+シス テム故障 から回復 せる異常	、 章 夏さ								
D.5.2.2					リ 境	Iハーサル環 ^竟		本番デー タ使用可 能						【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 数	Jハーサル回 対	リハーサ ル無し	1回	2回	3回	4回	5回以上								

*GE 377		-L	J# -	J	重複項	メトリクス			レヘ	ベル			運用スト・	_	社会	的影響が殆ど無いシステム	社会的	7影響が限定されるシステム T	社会的影	影響が極めて大きいシステム
負番	大項目	中項目	小項目	小項目説明	項目目	(指標)	0	1	2	3	4	5	の景響	<u>影</u>	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.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。				•		
D.5.3.1			しニゴッかか	移行中のトラブル時の対応体制や対応プラン		トラブル対処	坦宁無	対応体制	立方 体制					【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.3.3.1				参行中のドラブル時の対応体制や対応プラブ 等の内容。		の規定有無	祝足無し	めた体制 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 t			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、		順守すべき 社内規程、 ルール、法 令、ガイドライ		有り						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)	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。	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。	0 無し	ューザ要件に応じてレベルをする必要がある。
				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	0	ン等の有無								・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		[+] 順守すべき規程、法令、ガイドライン等が存在する場合		[+] 順守すべき規程、法令、ガイドライン等が存在する場合		[+] 順守すべき規程、法令、た ライン等が存在する場合
														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】						
	<u>_</u>													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。						
E.2.1.1		セキュリティ リスク分析	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。	0	リスク分析範 囲	分析なし	重要度を選出を変える。 のでは、一般では、一般では、一般では、一般では、一般では、一般では、一般では、一般	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。	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。	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		ネットワークを通じた、不特定の攻撃者からの脅威にさらさまた、重要情報が取り扱われるため、脅威が現実のものと場合のリスクも高い。そのたるステム全体のリスクを分析す要がある。 [-] データの移動や更新等がず、それらに伴なった情報へセス権限の変化等による脅威としない(あるいは許容する)
E.3.1.1		セキュリティ 診断	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		ネットワーク 診断実施の	無し	 有り						【メトリクス】 ネットワーク診断は、システムに対する広義の診断をあらわしている。 ネットワーク診断には、目視	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	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		ネットワークを介した、外部か 不特定多数の攻撃者からの
				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。		有無								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		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		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		さらされる。また、重要情報が扱われているため、脅威が現ものとなった場合のリスクも高そのため、ネットワークを由る
														も検討する。		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。		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。		撃に対する脆弱性を分析するがある。 [-] セキュリティに関する専門 知識を有する者により、ネット
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	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	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	1 有り	クを介した攻撃への対策が十 検討し、各種ドキュメントが作 ネットワークを通じた不特定 攻撃者からの脅威にさらされ
					0									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。		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		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		のため、Webアプリケーションする脆弱性を分析する必要かる。 [-] Webアプリケーションを用し
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。		場合		ない場合		場合
														【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	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		セキュリティリ スク見直し頻 度	無し	るイベント の発生時	セキュリティに関するイベントの発生時に実施(随					【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。						
				ホールや脆弱性、新たな脅威の調査等が含まれる。				時 <i>)</i> 	時) 十 定期的に 実施											
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												
E.4.2.1			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	高い資産	洗い出し た脅威全 体に対応											

【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。

			₩	i 重 夏 要 メトリクス	7		レ	ベル		運用	<u> </u>	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	が極めて大きいシステム
項番	大項目	中項目 小項目	小項目説明 「 ^個 項目	g g / (指標) g g (指標)	0	1	2	3	4	5 タ	<u> </u>	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.4.3.1		セキュリティパ・ チ適用	ッ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。	セキュリテ パッチ適用 囲	範 ティパッラ	重要度が 高い資産 を扱う範 囲、あるい は、外接	システム 全体							•			
E.4.3.2			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	セキュリティ パッチ適用 針	イ セキュリ 方 ティパッラ を適用しな	緊急性の	キュリティ	<u>ā</u>									
E.4.3.3			容として明記されることが望ましい。	セキュリテ パッチ適用 イミング	イ セキュリタ ティパッラ を適用した	障害パッ チ チ適用時 な 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						
E.5.1.1		アクセス・利認証機能	資産を利用する主体(利用者や機器等)を識	管理 権限 <i></i>	実施しな	10	複数回の	指粉 同			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。	1 I10 I	攻較老が管理族限を毛に入れるこ	1 2 複数回の	攻撃者が管理権限を手に入れるこ	2 複数回の 水酸	*老が答理族限を毛に入れる"
E.J.1.1		用制限	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。	持つ主体の認証		TEL	認証	複数目、 異なる方 式による 認証			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。		及事者が管理権限を予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	こでは一般の一般の一般の一般の一般の一般の一般の一般の一般の一般の一般の一般の一般の一	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。	認証 とに。 抗す する。 [-] タ 限を	はない。日本権限を手に入れるこよる、情報漏洩等の脅威に対でるため、複数回の認証を実行必要がある。 外部ネットワーク越しに管理権持つ主体がアクセスできないり場合
E.5.1.2				管理権限を持たない主の認証	実施しな体い	10	複数回の 認証	複数回、異なる方式による認証									
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。	システム上対策におけ、操作制限原	·る	が限がます。 要ののようでは、からないです。 がいた。 がいた。 がいた。 がいた。 がいた。 がいた。 がいた。 がいた					【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。	限のプログラムの グラムコ 実行、コ マンドの 操作、ファイルへの アクセス	不正なソフトウェアがインストールされる、不要なアクセス経路(ポート等)を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 (操作を制限することにより利便性や、可用性に影響する可能性がある)	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	不正なソフトウェアがインストールされる、不要なアクセス経路(ポート等)を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 (操作を制限することにより利便性や、可用性に影響する可能性がある)	限のプロ れる グラムの 等)を 実行、コ り、情 マンドの となっ 操作、ファ 等へ イルへの する。 アクセス (操作	はソフトウェアがインストールさ、不要なアクセス経路(ポートを利用可能にしている等によ 青報漏洩の脅威が現実のものってしまうため、これらの情報 の不要なアクセス方法を制限必要がある。 作を制限することにより利便性可用性に影響する可能性があ
E.5.2.2				物理的なタ		必要最小					【メトリクス】		[-] 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	=	[-] 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	なられ	重要情報等への攻撃の拠点と ない端末等に関しては、運用に 対策で対処する場合
E.3.2.2				物理的な業策による操制限度		必要 駅の ドウェアの 利用 作の 許可					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 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											
E.6.1.1		データの秘 データ暗号化 匿	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。	伝送データ暗号化の存無		認証情報 のみ暗号 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。	のみ暗号化	ネットワークを経由して送信するパスワード等については第三者に漏洩しないよう暗号化を実施する。 [-] 認証情報をネットワークを経由して送信しない場合	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) [一] 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	を暗号化 報にのデにより、 「一」 「対ル	カルネットワーク経由で重要情送付する場合においても、特要な情報については、盗聴等が成に対抗するために、伝送・タを暗号化する必要がある。送データを暗号化する可能性がある)生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い実施されている場合/クラーカットワーク上での盗聴の脅威いては許容する場合/機密性
E.6.1.2				蓄積データ		認証情報					【レベル1】		蓄積するパスワード等については	2 重要情報	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 データベースやバックアップテープ	は求 れる 2 重要情報 デー	さめられないが完全性が求めら 重要情報を扱う場合 ・タベースやバックアップテープ
				暗号化の存無		のみ暗号化					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。		第三者に漏洩しないよう暗号化を 実施する。 [-] 認証を実施しない場合	を暗号化	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ごとにより、性能に影響する可能性がある) [一] 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	を暗号化 等にパ の	格納されている個人情報等や ワード等の重要情報の漏洩の に対抗するために、蓄積デー 暗号化する必要がある。 債データを暗号化することによ 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 が、運用対策等の他の複数の対 より、安全性が確保されている が機密性は求められないが完
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、				全性が求められる重要情報を扱う 場合		が求められる重要情報を扱う

				重重加加加			レ	ベル			運用コ		社会的	内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
項番 大項目	申項目	小項目	小項目説明	in in in in in in in in	0	1	2	3	4	5	ー ストへ の影 響	備考	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.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。	口グの取得	実施しな い	実施する					グは個々 必要に応 ・ログイン ・操作ログ ・セキュリ ・通信ログ ・DBログ	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。 じて、ログと作業記録との突き合わせも行う。 /ログアウト履歴(成功/失敗) デ	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)		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		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						、】 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 を確認するメトリクス。	高い資産	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。	高い資産 を扱う範 囲、ある	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- ク)	無し 一	重要度が高い資産を扱う範囲、あるには、外接部分						な】 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 認するメトリクス。	高い資産を扱う範	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。	高い資産 を扱う範	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	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		重要度が高い資産を扱う範囲、あるいは、外接部分	Α.					な】 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 監視の範囲を意味する。	高い資産 を扱う範 囲、ある	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	高い資産 を扱う範 囲、ある	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。
E.7.1.6				確認間隔	無し	ティに関するイベント の発生時	サール サール サール サール サール サール サール サール サール サール	-			ンシデン また、常用 自動検知	】 「イに関するイベントとは、重要な脅威が発見された際や、サービス上の不具合等によりイトが発生した可能性がある場合を意味する。 特確認とは、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。 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 シトの発生時に実施(随時)に含まれる。						
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4 の利用の有 無		有り												
E.7.2.2				確認間隔	無し	ティに関するイベント の発生時	サールリック マイン マキュリック マイン マイン マイン で 大 で で ま で で ま で か か に い か か か に ま で か か に ま で か か に ま で か か に ま で か か に ま で か か に ま で か か に か に か に か か に か に か か に か か に か に か か に か か に か か に か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か に か か か に か か か に か か か に か か か に か か か に か か か か か に か か か か に か	-										
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 する必要	を実現する際には、ファイアウォール、 <mark>IPS、URLフィルタ、メールフィルタ</mark> 等の導入を検討	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		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 〇	無し	重要度が 高い資産 を扱う範 囲、あるい は、外接 部分					【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。	高い資産	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。	高い資産	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。	高い資産	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: 撃の回避	攻 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		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		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	マルウェア対象	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。	マルウェア家策実施範囲		重要度が高い資産を扱う範囲、あるいは、外接部分							高い資産		高い資産 を扱う範	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	高い資産	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

				重重複要メトリクス項項(指標)		l	ノベル			運用コーストへ		社会	的影響が殆ど無いシステム	社会的	り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
項番 大項目	中項目	小項目	小項目説明	項 項 (指標) 目 目	o	1 2	3	4	5	の影響	備考	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
.9.1.2				リアルタイム スキャンの実 施	実施しなまが	色する				リン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	レベル1】 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ッ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						
E.9.1.3				フルスキャン の定期チェッ クタイミング	(フ キャ える ング	ルス マンを行 らタイミ ががあ ば実施	1回/週	1回/日									
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	化	策の強				W	メトリクス】 /eb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 ・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 ・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 ・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。	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。	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関施する必要がある。
10.1.2				WAFの導入 の有無	無し有り	J					メトリクス】 IAF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。	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。 [+] 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		ッステムに侵入されることによる 情報の漏洩、踏み台等の脅威に 抗するために、機器による、侵入 止、検知を実施する必要がある。 [-] Webサーバへの対策、不正ア セス防止、ログの定期的な確認等 が実施されている場合
.11.1.1	セキュリティ インシデント 対応/復旧	シデント対応/	レ 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	J				せ の 【1 セ ま	メトリクス】 マ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)関係者に対するセキュリティ教育を実施する。 レベル0】 マ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】 「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 ボサービスを利用する場合も含まれる。						
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		(重	的有り 制約有 ¹ 要な制 (全ての のみ適 約を適所	制			【. シ り の ま 予	メトリクス】 ・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 、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)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。 に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 が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 きも制約条件となる。	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	(重要な制 約のみ道 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合、もしくは業界などの標準や取決めなどがない場合 [+] 法や条例の順守よりも高度な内基準の制約を受け、かつ、全に対応することが必要な場合
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		(重	的有り 制約有「要な制(全ての 別み適 約を適用	制					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	(重要な制	設置に関して何らかの制限が発生 引するセンターやマシンルームを前投 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	程 (重要な# 約のみ道 用)	設置に関して何らかの制限が発 するセンターやマシンルームを前 として考慮。ただし条件の調整な が可能な場合を想定。 [+] 設置センターのポリシーや共 運用など運用に関する方式が制 となっている場合
. .2.1.1	システム特 性	ユーザ数	ジ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 上原 ザのみ まっ	艮が決 不特定: oている 数のユ- ザが利)	-			B す 【I 前	重複項目】 .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であるとあるとめ、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】 が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		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	数のユーザが利用	・ 国民全体がアクセスする可能性 ・ あるような場合を想定。
7.2.2.1		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	特定クライ上原アントのみまっ	艮が決 不特定: っている 数のクラ アントが 用	5イ					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		また。 あらかじめ一定の値を決めて合意 することを想定。 [+] 上限台数を設定きない場合		また。 あらかじめ一定の値を決めて合意 することを想定。 [+] 上限台数を設定きない場合
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	牧拠点					レベル1】 U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。	1 複数拠点	複数拠点を想定。	1 複数拠点	複数拠点を想定。
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- 内	一都市 同一都 府県内	道 同一地方	国内	海外	レールま	レベル】 ・ベル5になると、多言語対応などの考慮も必要となる。 をた、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なる。	0 拠点内	[+] 複数拠点の場合 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	[-] 単一拠点の場合 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	[-] 単一拠点の場合 アクセス範囲は国内とすることを定。 [-] 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
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 〇	特定製品 一部 の指定が 定額 ない 指別 る	部に特 サポート 製品の 困難な動 定があ 品の指 がある	製						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		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 の指定か ない	合 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

百来	大項目	中項目	小項目	小項目説明	重重要	メトリクス			レ <i>・</i>	ベル T			運用スト	·へ 	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	が極めて大きいシステム
	八項口	丁块口			項目目	(指標)	0	1	2	3	4	5	の 響		選択レベル	選択時の条件	選択レベル	選択時の条件	選択レベル	選択時の条件
2.6.1			システム利用 氧 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	社内のみ	社外 (BtoB)	社外 (BtoC)										
.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。						
.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		UL60950 相当取得							0 規格取得 の必要無 し	ける。 機器の規格取得に関して指定がなまい場合を想定。		機器の規格取得に関して指定があった場合を想定。	の必要無 い場し	
.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、		規格取得の									0 規格取得	[+] 特に指定があった場合 引 特に制限などを受けない場合を想		[-] 特に指定がない場合 RoHS指令対応の装置が指定され	0 規格取得 特に	特に指定があった場合 :制限などを受けない場合
				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。		有無	の必要無 し 	相当取得							の必要無し	(+) 特に指定があった場合	令相当取 得 	た場合を想定。 [-] 特に指定が無かった場合	の必要無 定。 し [+] ‡	持に指定があった場合
.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		VCCI ClassA取 得	VCCI ClassB取 得											
1.1.1			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		耐震震度	対策不要	震度4相当 (50ガル)	 震度5弱相 当(100ガ	震度6弱相 当(250ガ	 震度6強相 当(500ガ	 震度7相 (1000ガ	当	【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	相当(10		相当(250		4 震度6強 震度 相当(500	
				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。	0				ル)	ル)	ル)	ル)		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。	ガル)	[-] 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		[-] 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		免震構造の建屋に設置で 屋環境と機器環境を総でする場合 時に震度7など強い地震 値が指定された場合
														【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。		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				
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		設置スペース 制限(マシン ルーム)	に関する	フロア設置 用機材を 用いて構 成	ント用機材					【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。		ウ 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	ント用機	ターでのラックマントをな 設置に関して制限がない
1.2.2				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(事務所 設置)	に関する	専用のス ペースを 割当て可	するス						1 専用の2 ペースを 割当て電	は、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。	2 人と混在 するス ペースに	端末機などフロントエンド業務用の 機材を想定。		機などフロントエンド業 を想定。
					0			能	設置必要					【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。	能	[-] 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	設置必要	[-] 業務的に人との混在が不要な 場合		業務的に人との混在が う
.4.2.3						並行稼働ス ペース(移行 時)	ペースの	共用ス ペースの 確保が可 能						【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。						
.4.2.4						設置スペース の拡張余地	張余地有 り		(特注対応 や工事が					【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。						
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		床荷重	2,000Kg/ ㎡以上	1,200Kg/ m [*]	800Kg/m²	500Kg/m ²	300Kg/m²	i 200Kg/n	m [*]	【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。	1					
				ど、設置のための対策が必要となる可能性が 高い。									C	【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。	j					
4.3.2						設置対策	不要	荷重を分 散するた めの資材	ラック当りの重量を	設置環境 固有の条										
								めの貧材 (鉄板など) を配備す る	制限して、 分散構成 を採る	所など)を 考慮して、 設置設計										
4.4.1			電気設備適合	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/		供給電力適	現状の設備で特に	電源工事	電源工事	を行う 工事など ができず	まったく対	<u> </u>			-					
				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		供給電力適 合性	制限無し	が、分電盤改造など二次側	が、一次、二次とも工事可能	規模に対して容量が少し足り	設置場所 を再考す る必要が									
				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。				の工事の みで対応 可能		ない	ある									
4.4.2						電源容量の 制約	(必要な電 源容量の	制約有り (既製品で 対応でき るレベル)	(カスタマイ ズや工事											
4.4.3						並行稼働電	能) 全面的に	部分的に	確保が困					【レベル2】 なにはこせに対象が必要な場合には、即今や集ませること、即次項目に D 1 1 2 E 40 2がま	-					
1111							確保が可能	能		10年月	1 口門	12田甲		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。						
7.4.4.4						停電対策	無し	瞬断(10ms 程度)	S 1073	1時間	日间	週間		【レベル1】 UPS, CVCFなど電源安定化の対策を検討する。						

社会的影響が殆ど無いシステム

選択時の条件

社会的影響が限定されるシステム

選択時の条件

選択レベル

社会的影響が極めて大きいシステム

選択時の条件

選択レベル

					重重	メトリクス			レ	ベル		1	運用コストへ		
番	大項目	中項目	小項目	小項目説明	項目目	(指標)	0	1	2	3	4	5	の影響	備考 	
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。	
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。	
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	32度(多く のテープ 装置の稼	5度から35 度(多くの 機器の稼 働可能条	0度~40度	0度~60度	E −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。	th
								働可能条 件)	1 11)					【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。	
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。	
.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	ポットなど	り、対策が					【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。	
.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)		ズや工事	,					
5.5.1.1		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		グリーン購入 法対応度	対処不要	準を満た す製品を	グリーン購入法の基準を満たす製品のみを使用	Ė					
F.5.1.2				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。		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。	
.5.1.3						機材のライフサイクル期間		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。	Š
.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		エネルギー消費の目標値	月 日標値無 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					【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。	
				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。					有る					【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			CO₂排出量	システムのライフサイクルを通じて排出される CO2の量。ただし、単純なCO2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		CO₂排出量の 目標値	目標値の 設定不要		提示が有り、更なる					【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。	
				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。					追加削減 の要求も 有る					【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】	
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		騒音値	対策不更	8748(井巨	85dB(茶压	80dB(英国	404B(図事	35dR/ 字字		【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。 【運用コストへの影響】	_
. J.4 . l				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。		神田 日 旧	A] 來个安	RoSPAの 騒音基準 による防 音保護具	RoSPAの 騒音基準 による第2 アクション	RoSPAの 騒音基準 による第1 アクション レベル)以 下	館レベル)			【連用コストへの影響】 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。	