

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに遡る)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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				【マトリクス】 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。	1	特定のサーバで冗長化	0	非冗長構成	
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)。	1	特定のコンポーネントのみ冗長化	0	非冗長構成	
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。	1	特定の機器のみ冗長化	0	非冗長構成		
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。	1	特定のコンポーネントのみ冗長化	0	非冗長構成		
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			【マトリクス】 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。	1	一部冗長化	0	冗長化しない			
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			【マトリクス】 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。	1	一部冗長化	0	冗長化しない			
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。	2	用途に応じて分割	0	分割しない			
A.2.6.1		データ	データの保護に対する考え方。	○		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。	2	オンラインバックアップ	2	オンラインバックアップ		
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	システム内の全てのデータを復旧			【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。	1	一部の必要なデータのみ復旧	1	一部の必要なデータのみ復旧			
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)			【マトリクス】 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。	1	エラー検出のみ	1	エラー検出のみ		
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		【マトリクス】 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	2	同一の構成でシステムを再構築		
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			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)			0	外部保管しない	0	外部保管しない			

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに連する)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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				【マトリクス】 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	1	特定の対策を実施する	1	特定の対策を実施する	
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	3	業務停止となる障害の全ての範囲	
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。 【マトリクス】 運用時間は、オンライン/バッチを含みシステムが稼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。	5	24時間無停止	4	若干の停止有り (9時～翌朝8時55分)	
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。 【マトリクス】 特定日とは、休日/祝祭日や月末月初など通常の運用スケジュールとは異なるスケジュールを定義している日のことを指す。特定日が複数存在する場合は、それぞれにおいてレベル値を整合する必要がある(例:「月～金はレベル2だが、土日はレベル0」、「通常はレベル5だが、毎月1日にリポートをするためその日はレベル3」など)。また、ユーザの休日だけでなく、ベンダの休日についても特定日として認識し、運用保守体制等を整合すること。	5	24時間無停止	3	1時間程度の停止有り (9時～翌朝8時)	
C.1.2.1					○		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。 【マトリクス】 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。	2	システム内の全データを復旧	2	システム内の全データを復旧	
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)				【マトリクス】 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。	3	データの長期保存(アーカイブ)	3	データの長期保存(アーカイブ)
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					○	【マトリクス】 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	2

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	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに遡する)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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			5	同期バックアップ	5	同期バックアップ
C.1.3.2			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まない。「E.7.1 不正監視」で別途検討すること。		○	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	リアルタイム監視(分間隔)
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う
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。	1	一部監視を行う	1	一部監視を行う

非機能要求グレード 2018 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	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに属する)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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。	3	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	1	サーバ機器のみ時刻同期を行う
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)	0	計画停止有り(運用スケジュールの変更可)
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。	2	1ヶ月前に通知	2	1ヶ月前に通知
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	1	一部の保守作業を自動で実行する
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、自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、配布と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。	2	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	2	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
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、自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、配布と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。	2	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	1	端末への更新ファイル配布機能を実装し、自動にて配布と更新処理を実行する
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。	1	一部のハードウェアにおいて活性保守を行う	1	一部のハードウェアにおいて活性保守を行う
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。	1	一部のソフトウェアにおいて活性保守を行う	1	一部のソフトウェアにおいて活性保守を行う
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		メーカーの必要回数。	1	年1回	1	年1回
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					2	(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	2	(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

非機能要求グレード 2018 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	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに含める)		
								0	1	2	3	4	5			調達仕様		調達仕様		
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、ユーザー側・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	3	
C.3.1.2																				
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る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。	0	障害復旧作業は全て手動で実施する	0	障害復旧作業は全て手動で実施する			
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	ユーザーの指定する時間帯(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。	2	24時間対応を行う	0	ベンダの営業時間内(例:9時～17時)で対応を行う			
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ーの翌営業日中	保守員到着が異常検知からユーザー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。	4	保守員到着が異常検知から数時間内	4	保守員到着が異常検知から数時間内			
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ーの翌営業日中	SE到着が異常検知からユーザー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。	4	SE到着が異常検知から数時間内	4	SE到着が異常検知から数時間内			
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。	2	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	2	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			
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					1	一部、予備機有り	1	一部、予備機有り			
C.4.1.1		運用環境	開発用環境の設置	ユーザーがシステムに対する開発作業を実施する目的で導入する環境についての項目。	○		開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する				【メトリクス】 開発用環境とは、本番環境とは別に開発専用を使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される開発フェーズの環境は、本項目に含めない。 【レベル】 開発フェーズでは開発環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの開発環境を設置しないを選択する。	1	運用環境の一部に限定した開発環境を設置する	1	運用環境の一部に限定した開発環境を設置する		
C.4.2.1			試験用環境の設置	ユーザーがシステムの動作を試験する目的で導入する環境についての項目。	○		試験用環境の設置有無	システムの試験環境を設置しない	システムの開発用環境と併用する	専用の試験用環境を設置する				【メトリクス】 試験用環境とは、本番環境とは別に試験専用を使用することのできる機材一式のことを指す。本番移行後に本番環境として利用される試験フェーズの環境は、本項目に含めない。 【レベル】 試験フェーズでは試験環境として使用していたが、本番移行後は本番環境となる環境については、レベル0のシステムの試験環境を設置しないを選択する。	2	専用の試験用環境を設置する	2	専用の試験用環境を設置する		
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	ユーザー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】 ユーザー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、ユーザー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。	1	システムの通常運用のマニュアルを提供する	1	システムの通常運用のマニュアルを提供する	

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに遡る)		
								0	1	2	3	4	5			調達仕様		調達仕様		
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。	1	構内LANを介してリモート監視を行う	1	構内LANを介してリモート監視を行う	
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					○	【マトリクス】 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	2	任意のリモート操作を行う	
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					【マトリクス】 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。	2	社外の外部システムと接続する	2	社外の外部システムと接続する
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。	2	新規監視システムに接続する	2	新規監視システムに接続する	
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。	1	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う	1	ベンダの自社製品（ハードウェア）に対してのみ保守契約を行う		
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。	1	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う	1	ベンダの自社製品（ソフトウェア）に対してのみ保守契約を行う		
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				【マトリクス】 ここでのライフサイクルとは、次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	3	10年以上		
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						1	一部ユーザが実施	1	一部ユーザが実施		
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						1	一部ユーザが実施	1	一部ユーザが実施		
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						0	常駐しない	0	常駐しない		
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				4	24時間対応	4	24時間対応				

非機能要求グレード 2018 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	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに含める)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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					4	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	4
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。	1	オンコール待機	1	オンコール待機
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					4	1ヶ月以上	4
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					2	1週間以内	2
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					2	一部ユーザが実施	2	一部ユーザが実施
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。	3	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	3	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
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						2	定期開催	2	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	4	月1回
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	3	障害および運用状況報告に加えて、改善提案を行う
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	1	既存の社内規定に従って、内部統制対応を実施する
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。	1	既存のサービスデスクを利用する	1	既存のサービスデスクを利用する
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。	1	既存のインシデント管理のプロセスに従う	1	既存のインシデント管理のプロセスに従う
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。	1	既存の問題管理のプロセスに従う	1	既存の問題管理のプロセスに従う
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。	1	既存の構成管理のプロセスに従う	1	既存の構成管理のプロセスに従う
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。	1	既存の変更管理のプロセスに従う	1	既存の変更管理のプロセスに従う

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク	OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに達する)
								0	1	2	3	4	5			調達仕様	調達仕様
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					【マトリクス】 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。	1 既存のリリース管理のプロセスに従う	1 既存のリリース管理のプロセスに従う
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	1 3ヶ月未満
D.1.1.2							システム停止可能日時	制約無し(必要な期間の停止が可能)	5日以上	5日未満	1日(計画停止日を利用)	利用の少ない時間帯(夜間など)	移行のためのシステム停止不可		【マトリクス】 システムによっては、システム停止可能な日や時間帯が連続して確保できない場合がある。(例えば、この日は1日、次の日は夜間のみ、その次の日は計画停止日で1日、などの場合。) その場合には、システム停止可能日とその時間帯を、それぞれ確認すること。 【レベル】 レベル0はシステムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。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。	5 移行のためのシステム停止不可	3 1日(計画停止日を利用)
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。	1 有り	0 無し
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・機器のシステム全部を入れ替える	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。	3 移行対象設備・機器のシステム全部を入れ替える	3 移行対象設備・機器のシステム全部を入れ替える
D.4.1.2		移行対象(データ)	移行データ量				移行データ形式	移行対象無し	移行先と形式が同一	移行先と形式が異なる					【マトリクス】 データ形式は、アプリケーションに依存したフォーマット、テーブル形式や文字コードなど、新システムに移行するために考慮すべきデータ形式のパターンを指す。 【レベル】 移行データ形式のパターンが複数ある場合には、それぞれについてデータ形式を確認すること。	2 移行先と形式が異なる	2 移行先と形式が異なる
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	ユーザとベンダで共同で実施	全てベンダ					【マトリクス】 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。	1 ユーザとベンダで共同で実施	1 ユーザとベンダで共同で実施
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				2 全ての正常ケース	2 全ての正常ケース
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。	2 対応体制と対応プランの規定有り	2 対応体制と対応プランの規定有り
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例) ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール			順守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り						【マトリクス】 規程、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。 例) ・国内/海外の法律 不正アクセス禁止法・不正競争防止法・プロバイダ責任法・改正個人情報保護法・SOX法・EU一般データ保護規則(GDPR)・特定電子メール送信適正化法・電子署名法 など ・資格認証 プライバシーマーク・ISMS/ITSMS/BCMS/CSMS・ISO/IEC27000系・PCI DSS・クラウド情報セキュリティ監査・TRUSTe など ・ガイドライン FISC・FISMA/NIST800・政府機関の情報セキュリティ対策のための統一基準 など ・その他ルール 情報セキュリティポリシー など 【レベル1】 構築するシステムが関係する国や地域によって、順守すべき法令やガイドラインが異なることに注意すること。	1 有り	1 有り
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	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

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに連する)	
								0	1	2	3	4	5			調達仕様		調達仕様	
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	2	システム全体
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						1	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	1	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
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	1	有り	
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、ウイ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						1	重要度が高い資産を扱う範囲、あるいは、外接部分	1	重要度が高い資産を扱う範囲、あるいは、外接部分
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	1	緊急性の高いセキュリティパッチのみ適用
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】 パッチが出荷し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。	1	障害パッチ適用時に合わせて実施	1	障害パッチ適用時に合わせて実施		
E.7.1.1		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。			○	ログの取得	実施しない	実施する				【マトリクス】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。取得したログは個々のログを確認するだけでなく、複数のログを組み合わせて相関分析することも検討する。 必要に応じて、ログと作業記録との突き合わせも行う。 ・ログイン/ログアウト履歴(成功/失敗) ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ等	1	実施する	1	実施する	
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		1	1年	3	5年
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					0	無し	0	無し	
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				0	無し	0	無し
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	1	有り	
E.8.2.1			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。			○	不正通信の検知範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体			【マトリクス】 検知範囲の設定に応じて、IDS等の導入を検討する必要がある。	1	重要度が高い資産を扱う範囲、あるいは、外接部分	1	重要度が高い資産を扱う範囲、あるいは、外接部分	
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア(ウイルス、ワーム、ボット等)の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。 対策を実施する場合には、ウイルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。			○	マルウェア対策実施範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	重要度が高い資産を扱う範囲、あるいは、外接部分	1	重要度が高い資産を扱う範囲、あるいは、外接部分	

非機能要求グレード 2018 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	マトリクス (指標)	レベル						運用コストへの影響	備考	指令システムおよび指令系ネットワーク		OAシステムおよび支援系ネットワーク (指令システムとリアルタイム連携必要な範囲は指令システムに達する)		
								0	1	2	3	4	5			調達仕様		調達仕様		
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						【マトリクス】 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	1	有り	
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)					【マトリクス】 システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発環境を整備する必要がある。 また運用予定地での構築が出来ず、別地にステーjing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)	2	制約有り(全ての制約を適用)	
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)	2	制約有り(全ての制約を適用)		
F.2.1.1		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数。		○	○	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用					【重複項目】 B.1.1.1。ユーザ数は性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもあるため、性能・拡張性とシステム環境・エコロジーの両方に含まれている。 【レベル】 前提となる数値が決められない場合は、類似システムなどを参考に仮の値でも良いので決めておくことが必要。	0	特定ユーザのみ	0	特定ユーザのみ
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						0	特定クライアントのみ	0	特定クライアントのみ
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	1	複数拠点
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)					0	部門内のみ	0	部門内のみ
F.4.2.1	機材設置環境条件	スペース	スペース	どの程度の床面積(WxD)/高さが必要かの項目。保守作業用スペースについても考慮する。また、移行時には新旧システムが並行稼働可能なスペースの確保が可能か否かについても確認が必要である。可能であれば事前確認を実施する。		○	設置スペース制限(マシンルーム)	スペースに関する制限無し	フロア設置用機材を用いて構成	ラックマウント用機材を用いて構成					【マトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。	2	ラックマウント用機材を用いて構成	2	ラックマウント用機材を用いて構成	
F.4.2.2						○	設置スペース制限(事務所設置)	スペースに関する制限無し	専用のスペースを割当て可能	人と混在するスペースに設置必要					【マトリクス】 具体的な面積と高さも併せて確認する。また、スペース形状や場所による耐荷重の差異にも留意すること。 【レベル】 設置スペース制限は前提条件として既に規定されていると捉え、その要求に対してシステムを設置する場合の難易度をレベルとしている。スペース確保の視点での難易度ではないことに注意。	2	人と混在するスペースに設置必要	2	人と混在するスペースに設置必要	
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					【マトリクス】 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。	1	共用スペースの確保が可能	1	共用スペースの確保が可能	
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)					【マトリクス】 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。	2	制約有り(特注対応や工事が必要)	2	制約有り(特注対応や工事が必要)	