学校ネットワークシステム再構築及び運用保守業務　サービス仕様書

【注意事項】
・「実施内容の例」については、あくまでサービス仕様の理解を助けるための例示であり、
これらの実施を提案の前提とするものではなく、また、これらの実施が、サービス仕様を満たす条件ではないことに留意すること。

サービス分類			サービス仕様	サービス仕様の補足	実施内容の例
1.事業実施全般					
	1.1 基本事項				
		1.1.1	関係者と十分なコミュニケーションを図り、サービスの最適化のために必要な措置を取ること。	コミュニケーションは文書によるものを原則とする。	プロジェクト体制における会議体・メンバー・コミュニケーション文書・承認権限・開催頻度等を委託者側の会議体も含め示し、提示する。
		1.1.2	本事業の品質改善又は効率化を図るための改善計画を立案し、これを自ら実施するほか、必要な事項については、委託者に改善提案を行うこと。	改善提案の範囲には、本事業に関係しない事項も含むことができる。	
	1.2 事業継続性				
		1.2.1	事業の完了時、及び破綻時において、サービスの継続性を確保するための計画を策定し、最新の状態を維持すること。	本事業の完了時、及び事業者が破綻した場合、構成企業や製品提供元が破綻した場合等、事業やサービスの継続に支障を来たす場合を想定し、具体的な対応方法を策定しておくこと。なお、対策に要する費用は原則本事業の範囲内であることに留意すること。	保険に加入し、保険のカバー範囲と、それ以外の範囲に分けて対策を立案する。
		1.2.2	災害時におけるサービス継続を確保し、継続計画を策定・実施すること。実施内容は常に確認・検証が可能であること。	大規模災害によりサービス提供が困難な事象が発生した場合、発生時から①1週間以内、②1ヶ月以内、③1ヶ月以降、に分類し、それぞれのフェーズにおけるサービスの提供方法を策定すること。 少なくとも、①及び②の対策・対応については、本事業の範囲内とし、③においては、災害発生前と同等の業務レベルを維持できるサービスを提供するために必要な具体的な対策を示し、想定費用を積算すること。	
2 システムの性能					
	2.1 稼働時間				
		2.1.1	事業関連図書もしくはプロジェクト計画書で特に指定する場合を除き、稼動時間は、24時間365日とする。また、業務時間は、土・日曜日と祝祭日、および12月29日から1月3日を除く全ての日で原則8:30～17:30とする。	稼働時間・業務時間については、委託者からの申し出・協議により変更する場合もある。	
		2.1.2	メンテナンス等により予定されたシステムの計画停止時間の総計は、年間総稼動時間の5%以下であること。また、一回の停止時間については、委託者の承認を得て決定すること。	稼働時間内に、利用者に何らかの影響のある機能等が計画的に提供されない状態を、計画停止とみなす。 稼働時間外における停止時間は、計画停止時間に含まない。 計画停止時は、作業計画書によりシステム停止予定時間を明らかにした上で委託者の承認を得ること。	
		2.1.3	予定外のシステム停止時間の総計は、総稼動時間の1%以下であること。	稼働時間内に、利用者に何らかの影響のある機能等が予定されずに提供されない状態を、予定外停止とみなす。 復旧のために稼働時間内に影響を与えた部分を除き、稼働時間外における停止時間は、予定外停止時間に含まない。	
	2.2 性能				
		2.2.1	通常想定される業務実施に支障の出ない性能を維持すること。 要件を満たせない場合、もしくは委託者が満たせない可能性が高いと指摘した場合は、必要な措置を取ること。	性能の想定に際し前提となる端末性能、配置、使用方法、ネットワーク条件等について明示すること。対応可能な最大端末数等についても明示すること。 システム構築時の検証により、あらかじめ検証を行い、検証結果について委託者の承認を得ること。 運営期間中についても適宜必要に応じた検証を実施すること。	
		2.2.2	運用管理期間内の使用ハードウェア容量・必要性能について予測を行い、十分な容量及び性能をあらかじめ確保しておくこと。	ハードウェア、サーバ関連設備、システム領域等、サービス仕様と業務仕様を満たすために必要なレベルまでは、事業者負担で必要な調達・作業・検査・メンテナンス等を行うこと。 ハードウェア等の資産を委託者は保有しないため、事業者の任意の提供形態を採ることができる。なお、サービス仕様等を満たすことができれば、ハードウェア等は新品である必要も最新である必要も無い。 あらかじめサービスの利用量やリソースの使用量についての予測を行い、運営管理期間中における計画を立案しておくこと。	運営管理期間中のデータ容量・トランザクション予測を行い、必要に応じてハードウェアを容易に追加・交換、設定できるスキーム（仮想化等）を用意しておく。 リソースの予測について複数パターンを想定し、対応策を立案する。
3.マネジメント					
	3.1 基本事項				
		3.1.1	十分なコミュニケーション活動とレビュー活動を行い、プロジェクトの状況や品質をメンバー間で適時把握できるマネジメントを実施すること。	マネジメントはドキュメントベースで行い、委託者との協議事項や合意事項、要望事項などをすべて記録・管理すること。 タスクやToDoを管理し、進捗や品質をレビュー者が常に把握すること。	プロジェクトの状況やドキュメントをシステム的に管理するツールを導入する。
		3.1.2	プロジェクトに必要なリソースは、委託者分も含めて把握・管理をし、プロジェクトに支障をきたさないようにマネジメントすること。	委託者が行うべき作業、決定すべき事項は前もって具体的に通知すること。通知にあたっては、期間・人員・場所等について、十分可能な計画であるよう配慮すること。	プロジェクト全体の人員等のリソースを管理する責任者・ツールを設置し、投入する要員等のスキル・作業品質について常にレビュー・チェックを行い、委託者に報告する。
		3.1.3	月次及び年次で実績報告を行うこと。		
	3.2 進捗･品質管理				
		3.2.1	プロジェクトに関連する全ての作業について、マイルストーンを設置し、詳細な作業単位まで分解されたWBSによる管理を行うこと。	全ての作業について作業責任者及び成果物を明示し、作業内容を説明すること。 フェーズやタスク毎の完了基準を明確にすること。 作業期間が長期（2週間以上）となるものは複数に分解すること。 作業内容、成果物、担当者、予定開始日・終了日、実績開始日・終了日、予定工数、実績工数、は最低限管理・提出すること。	
		3.2.2	品質の管理は、可能な限り測定可能な定量値によって行うこと。	品質管理指標だけではなく、セットアップ・テストに関する指標も管理する。 また、SIサービス等に関連した品質管理指標についても考慮すること。	開発時間と（原因別の）修正時間との比率を管理し、手戻り率やその原因を分析する。
		3.2.3	プログラムやドキュメント等の成果物については、内部での検査・管理フローを明確にし、ミスの発生や品質の劣化を防止すること。	作業ミス、伝達ミス、レビュー漏れ等による品質問題を可能な限り最小化するための取り組みを実施し、常にチェック・更新を行う。	ユーザによる、現状業務との適合性レビューのための手法・プロセス・ツール等を提供し、チェックを行う。
	3.3 課題･リスク管理				
		3.3.1	プロジェクトに関する課題・リスクを常に管理し、リスクが顕在化する可能性がある場合は前もって通知すること。	リスクを内部的に管理するだけではなく、委託者と常にコミュニケーションを取り、必要な場合は委託者へも前もってリスク対策を要求しなければならない。	リスク管理・課題管理表を整備し、内容・対応者・履歴を含め管理する。
		3.3.2	プロジェクトに関するリスクを回避・低減できるよう、常に検討を行い、対策を提案すること。	本事業の対象範囲外であっても、影響を及ぼす可能性があれば積極的に通知・対策の提案を行うこと。 バックアップ方法やセキュリティ等のリスク対策を、委託者側が監査を行うことが可能であるように、システム及びドキュメント等の整備を行っておく。	プロジェクトメンバーから、リスクとなる可能性がある事項を吸い上げ、検討する仕組み（会議・ツール等）を設ける。

サービス分類			サービス仕様	サービス仕様の補足	実施内容の例
4 SIサービス					
	4.1 基本事項				
		4.1.1	各種仕様書、提案書、プロジェクト計画書等の要件を満たすシステムを構築し、運営すること。 要件を満たせない場合、もしくは委託者が満たせない可能性が高いと指摘した場合は、必要な措置を取ること。	業務要件の充足度を確認・検討する手法を提供すること。	
		4.1.2	プロジェクト計画書、要件定義書、テスト計画書、移行計画書、運用計画書、障害対応計画書等の重要なドキュメントの整備・最新化を行い、履歴を管理すること。	プロジェクト開始後に合意された事項があれば、随時適切なドキュメントへ追記し、参照が必要なドキュメントの分散化を招かないこと。 重要なドキュメントには変更履歴を記載した上で版数管理を実施し、提出すること。	ドキュメント管理手法・管理ツールを提供する。 ドキュメントの作成内容及び変更内容を確認する際、責任者・担当者が明確となるよう管理する。
		4.1.3	プロジェクトのメンバーは十分に能力・経験のある人員によって構成し、リーダークラスについては、氏名と経験・能力を示した上で、委託者の承認を得ること。	主要なマネージャ・リーダーの交代がある場合には、代替要員の審査を委託者が行い、合格した場合のみ、交代を許可する。 構築フェーズにおいては、原則交代を認めない。	
	4.2 システムの構築				
		4.2.1	システムに採用する製品やプログラムの詳細を十分に理解し、要件を十分に満たす機能・性能のシステムを提供すること。	要件を満たす機能・性能を実現できない場合、もしくはその可能性が非常に高いと委託者から指摘された場合には、必要に応じシステム構成やプログラムを変更すること。 委託者の業務を理解し、業務を効率的に実施できる処理手法を提案すること。	業務範囲を定義・確認するための手法・ツールを提供し、定期的に、開発対象範囲・業務要件を委託者と確認する。
		4.2.2	テストにあたっては、事前にテスト計画書を提示し、システムの利用開始前に十分なテスト期間を確保し、信頼性を確保すること。	利用開始後であっても、テスト不足と合理的に認められる場合には、必要なテストを実施すること。	テスト方針・テスト完了条件・合格基準について、本プロジェクト用の基準を作成し、関係者で共有する。
		4.2.3	業務に必要なデータは、既存システムからの移行もしくは入力等、必要な手法によって用意すること。	データ移行作業は原則として事業者で実施すること。	
	4.3 システムの運営				
		4.3.1	要件を満たす機能・性能等の品質を維持するために必要なシステム及びサービスを継続して提供すること。	運営管理期間中、要件や品質を維持するために必要なシステムの更新・バージョンアップ・プログラムのメンテナンス等を行い、正常な稼動を保証すること。 提供する製品等は、必ずしも最新のものである必要はなく、事業者の保証が得られれば、製造元の保証が必須でない場合もある。 対策を実施する際には、事前検証を必ず実施すること。	
		4.3.2	運営管理期間において、システムのノウハウを維持し、品質が低下しないよう、適切な措置を取り、定期的に報告すること。	プロジェクトマネジャー等、主要なメンバーの変更によりこれまでの経緯やノウハウが失われ、SI品質が低下するリスクがあるため、単純な引継ぎの充実以外に、ドキュメントやノウハウの蓄積や教育、ツールの利用等の手法を最大限活用し、SI品質が低下しないよう保証する。	技術的・業務的ノウハウ等をドキュメント化し、メンバーへの教育を継続して実施する。 変更管理や、委託者からの要望等の情報を共有できる体制・業務フローを整備する。
	4.4 ヘルプデスク				
		4.4.1	平日8:30～17:00の時間帯において、ヘルプデスクを準備すること。 時間外おいては、サービスに関する問合せの受付は可能であること。	システムの利用方法や障害問合せ、機器故障に対して、ヘルプデスクを適切に運用すること。	
		4.4.2	平日8:30～17:00の時間帯において、応答率は100%を確保すること。 定期的に利用満足度に関する調査を行い、満足度が不満足度を上回ること。	一線解決率を高める工夫を行うこと。 管理保全要員及び応答体制について確立し、対応に遅延をきたさないこと。	
	4.5 障害対応				
		4.5.1	平日8:30～17:15の時間帯に、利用者に影響を与える障害が発生した場合は、発生から10分以内に委託者へ通知し、発生から2時間以内に影響範囲の特定及び復旧予定時間の予測を行い、委託者へ報告すること。	障害の検知・通知方法と復旧手法を、障害のタイプ別に明示すること。 障害の切分プロセスを詳細に定義し、障害対策のためのドキュメントを整備し、検証を行うこと。	近郊にサービス拠点を用意する。 障害検知・通報スキームを導入する。
		4.5.2	平日8:30～17:15の時間帯においては、障害連絡の受付後2時間以内に現地かけつけによる復旧対応を行うこと。その時間帯以外に受付けた件については、直近のかけつけ保守対応時間にて対応すること。	電話連絡を常に受付けられる体制を整備すること。また、緊急時については、24時間の受付体制を整えること。 かけつけ時間が順守できない状況にあるときには、事前に委託者に連絡し、承認を得ること。	
		4.5.3	問題の事前検知が可能となるよう、各種サービスの稼働状態を監視すること。 問題の事後調査が可能となるよう、エラーログ・アクセスログ等システムの稼動に関する記録を残すこと。	ハードウェア的な稼働状態だけでなく、ソフトウェアサービスが正常に稼働しているかどうか検知できること。 ログ採取の方針を明示し、分析方法について提示すること。	開発標準の一部として、ログ記録・管理の基準を設ける。
	4.6 セキュリティ対応				
		4.6.1	事業期間を通じて、その時点において有効と判断される技術的・業務的・社会的それぞれのセキュリティ防御手段を備えること。 また、システムが危殆化したと判断される場合には、委託者へ報告し即時にシステムを停止すること。	不正なアクセス・ソフトウェア・システム利用を検知し、防御する仕組みを備えること。 パスワードその他の認証手段を整備し、適宜変更・見直しを行うこと。 不正なデータの出力・持ち出しを防止するための技術的手法を備えること。 不正なアクセス・システム利用があったかどうかを全て記録し、通知する手段を備えること。 疑わしいシステム利用記録を抽出できること。	端末に不正なソフトウェアがインストールされているかどうか検知する仕組みを備える。 不要なサービスを停止する。 事業者全体の取り組みとして、セキュリティ関連情報の調査・検証を継続して実施する。