別　紙

しずおか中部連携中枢都市圏事業　テレワーカー育成事業
システム保守業務仕様書

1.　システム運用管理の概要

当事業の目的や役割、実際の業務との関連を十分に認識し、運用期間中に求めるサービスレベルを満たす安定したシステムの運用を管理・統括する。

2.　本件の業務名・内容

No.	業務名	業務内容
1	e ラーニングシステム	・ソフトウェア保守
2	運用サポート	・システム・デザイン保守 ・問い合わせ対応
3	データセンターサーバ保守	・WEB サーバ管理 ・レンタルサーバ契約維持 ・サーバ監視 ・SSL サーバ証明取得維持 ・プライマリ DNS 管理

3.　業務履行期間

契約締結日から平成 31 年 3 月 31 日

4.　サーバ設置場所

受託者が契約するサーバ上においてサービスを提供する。

5.　サイトの運用

（1）サービスレベル

下記のサービスレベルを達成すること。サービスレベルは、協議の上、合意を得たときは変更することができる。なお、委託先におけるサーバのセキュリティについては、契約内容に考慮し、ソフトウエア及びハードウエアにおいて万全の対策が行われているかを確認すること。

種別	項目	内容	基準値	備考
可用性				
	サービス稼働時間	計画停止・定期保守を除くサービス期間を利用できる時間	24 時間 365 日　※災害時など不可抗力発生時を除く	
	サービス稼働率	計画停止・定期保守を除くサービス期間における稼働率	年間 99.9%以上　※災害時など不可抗力発生時を	

種別	項目	内容	基準値	備考
			除く	
	計画停止予定通知	点検・保守に係る定期的な停止に関する事前連絡	２週間前までに通知	
	システムメンテナンス	システムメンテナンスを実施するタイミング	月 1 回、平日 18：00～翌 8：00 の時間帯	
信頼性				
	障害対応	保守管理者の障害認知日時から、発生を委託者へ通知するまでの時間	12 時間以内	
		保守管理者の障害認知日時から、復旧予定日時を委託者へ通知するまでの時間	12 時間以内	
		保守管理者の障害認知日時から、復旧を委託者へ通知するまでの時間	12 時間以内※重大障害の場合は 24 時間以内	
		バックアップ	日次 5 世代分を深夜帯に取得	
		リカバリ	障害発生時の直近バックアップデータまで復旧	
	システム監視	システム監視の周期と手法	24 時間・365 日機械監視	
	不正アクセスの監視	保守管理者の不正アクセス認知日時から、発生を委託者へ通知するまでの時間	12 時間以内	
		保守管理者の不正アクセス認知日時から、対応着手するまでの時間	1 時間以内	

（2）運用業務

（1）の要件を満たすため、次に示す運用業務を日常的に実施し、システムが安定して提供されるよう努める。

業務	内容
システム監視業務	本システムの安定稼動を実現するため、稼動状況を日常的に監視する
障害管理業務	障害が発生した場合、早期回復を目的とし的確な障害対応を実施する

データ管理業務	障害やセキュリティインシデントに備え、バックアップデータを定期的に取得するとともに、適切に記録、保管する
システム保守・維持管理業務	本システムで使用している製品やモジュールを定期的に保守点検し、状態を把握するとともに、安定的に稼動するために必要な対応を実施する
構成管理業務	本システムの運用維持管理を効率的かつ効果的に行うため、システム資産を台帳に登録し管理するとともに、情報システム文書は適切に管理、保護する
サポート業務	本システム、ネットワークに関する問い合わせ対応を実施する

6.　システム監視

（1）概要

各システム・ネットワークについてサービスレベルを満たす安定した稼動を実現するため、各システム・ネットワークに発生したシステム障害の検出及び障害要因の事前検出、障害検出時の障害箇所や影響範囲の特定、またセキュリティインシデントの検出及び侵害箇所や影響範囲の特定を迅速かつ的確に行うことを目的とし、本システムの稼動状況を監視する。

（2）障害管理

システムについてサービスレベルを満たす安定した運用を求められている稼働時間中、提供し続ける事を基本方針とするが、万が一障害が発生した場合、早期回復を目的とし的確な障害対応を実施する。なお、障害が長時間に及ぶと判断されたときは、バックアップの復元等、サービスの停止範囲を最小化するとともに、サービスが利用できない旨の告知を必要な対象者に対して確実に行う。なお、障害発生時は、別に定める運用体制図に基づき対応を行う。

ア　業務範囲

業務	内容
障害対応	・障害一次切り分け ・障害回復作業
障害管理	・障害連絡及び状況連絡 ・障害対応の進捗管理 ・原因分析及び再発防止策検討・報告 ・各種マニュアルの現行化管理

(ア)業務内容

①　障害対応

・アラート・報告をもとに、システム・ネットワークの障害レベルを迅速かつ正確に

判断を行う。障害発生後は、システム運用マニュアルに従い、迅速かつ正確に回復作業を行い、二次障害の発生を防ぐ。

・障害に伴って、ハードウエア故障やソフトウエアの障害が発見された場合は速やかにハードウエア保守・ソフトウエア保守の内容に基づいたサポート手続きをとる。

・障害発生から復旧までの一連の障害対応については障害ごとに対応内容を経験として管理・共有・蓄積し、参照を行えるようにすることで、以後の障害発生の予防と発生時の円滑な障害対応を行う。

② 障害管理

・体制図及び障害管理フローを作成し、障害検知時に、迅速かつ確実に関連部門へ連絡する。作成した体制図及び障害管理フローは適宜更新を行う。

・障害復旧に向けた各種作業について、状況を把握して進捗を管理する。

・復旧した障害について情報を分析し、障害発生原因の特定、再発防止策の検討を行う。再発防止策については随時障害対応結果と共に報告すると共に、必要に応じて定例会にて報告すること。

・障害分析に基づき、障害発生を予防する、または発生時の対応事項については、適宜共有してサービスレベル向上に努める。

7. 個人情報の取り扱い

本サイトにおいて取得する、登録者等の個人情報については、サーバ上で管理する。委託者の許可なくダウンロード等によりサーバ上からデータを取り出すことは一切認めない。

8. バックアップデータの管理

（1）概要

システムに障害が発生した時に備え、速やかにリカバリを行うため、各システムとデータのバックアップを行う。なお、詳細設計段階においては、リカバリの実行時間が、サービスレベルの範囲内で復旧が完了するよう、リカバリとバックアップ設計を行う。また、バックアップ実行時に、要求するサービスレベルの範囲で稼働している他システムへ影響しないような詳細設計を行う。

（2）リカバリ

各システム・ネットワークへ障害発生時に、サービスレベルに定める障害回復時間内で速やかに回復できるよう、詳細設計段階で設計を行う。

ア 障害時のリカバリ

障害発生時に必要な場合、サーバのシステムやネットワーク機器設定、データのリカバリをバックアップから行い、正常に動作可能か検証を行い、障害回復を図る。

（ア）セキュリティインシデント時のリカバリ

セキュリティインシデントの事実を解析し、対処を検討する。

イ　バックアップ

システム障害発生時に、サービスレベルに定める障害回復時間内で速やかにリカバリが行えるよう、詳細設計段階でシステムとデータのバックアップ設計を行う。

（ア）データバックアップ

障害により各システム・ネットワークが扱うデータが破損した場合に、可能な限りデータを障害直前の状態まで戻すためにデータのバックアップを行う。

①　システムバックアップ

システムの障害発生時の復旧作業を迅速に実施するために、最新の状態のシステムのバックアップを行う。

（3）媒体の保管・破棄

バックアップ媒体の保管・破棄については、保管中のバックアップの破損、バックアップに含まれるデータが漏洩しないよう詳細設計段階で設計を行い運用管理マニュアルに記載し、それに沿って適正な運用を行う。

9.　システム保守・維持管理

（1）概要

システムのサービスレベルを満たす安定した運用を実現するために、本システムで使用している製品やモジュール及びネットワーク機器に対して定期的に点検、保守作業を行う。また、セキュリティパッチの確認と適用、ウィルス定義ファイルの更新確認などの安定運用に必要な運用業務を行う。

（2）日次点検

故障を早期に発見するため、定期的に外部からのサービス利用可否確認などの点検作業を実施する。項目については、サービスレベルを満たせるよう、詳細設計段階で設計を行い、それに従い点検を行う。

（3）定期保守

システムを安定して稼動させるために、定期保守を実施する。なお、緊急性を伴わないセキュリティパッチ、更新されたファームウェアなどの各種アップデートの適用については、この保守点検作業の一部として適用作業を実施する。なお、作業に必要な場合、サーバ、ネットワーク機器、クライアント機器の計画停止を行うこと。詳細についてはサービスレベルを満たせるよう、詳細設計段階で設計を行い、保守時実施項目を運用管理マニュアルに記載し、それに従って点検を行う。

（4）臨時保守

システムに対して、公開された脆弱性を解消するために、緊急性の高いセキュリティパッ

チ、更新ファームウエアなどの緊急アップデートが公開された場合は、適用作業を実施する。

（5）ウィルス定義ファイルの更新確認

ウィルス定義が最新の定義ファイルに自動的になっていることを確認し、最新の定義ファイルになっていない場合は定義ファイルの更新を実施する。また、ウィルスの検知状況も併せて確認する。

（6）セキュリティパッチ情報の収集

セキュリティパッチ情報を第三者機関からの情報を収集し、早期発見・早期対処を行う。また、各構成機器メーカー、導入ソフトウエアベンダーが提供しているセキュリティ情報についても可能な限り収集する。各メーカーからの情報に加えて、ＩＰＡ（情報処理推進機構）の緊急対策情報・注意喚起情報、ＪＰＣＥＲＴ／ＣＣ（ＪＰＣＥＲＴコーディネーションセンター）の注意喚起、脆弱性関連情報の発表についても影響を確認する。

（7）アップデートの適用

ア　ファームウエアやセキュリティパッチなどのアップデートの適用は、システム安定稼動への影響と緊急度を判断し実施する。

イ　緊急度が高いアップデートについては、臨時保守作業を行い、実施する。

ウ　再起動を伴うアップデートの適用は、システムの稼働時間外又は、定期計画停止の時間帯に行う。なお、緊急性を伴う適用については委託者と協議のうえ臨時計画停止を設け作業日時を決定する。

（8）ＳＳＬサーバ証明書の更新

年１回程度、ＳＳＬサーバ証明書の更新作業を行う。

（9）計画停止

保守・点検等を実施するため、または電源、外部回線等システム外要因のため、あらかじめ決定した日時に計画的にネットワーク及びシステムを停止する。計画停止には、システム運用を円滑に実施するために定期的に停止する「定期計画停止」と外的要因によって臨時的に停止する「臨時計画停止」がある。

大区分	小区分	内容
定期計画停止	定期点検	安定稼動のためにネットワーク及びシステムを対象に実施する定期的な保守点検等
	予防保守	セキュリティの確保等安定稼動のために実施するソフトウエア及びファームウエアのバージョンアップ作業等
臨時計画停止	セキュリティ保守	セキュリティ確保のために実施するパッチ、フ

		ァームウエアのバージョンアップ作業等
	サービス機能保守	パフォーマンス改善等の目的で実施するネットワークの構成変更作業及び利用者の要望によりソフトウエアのカスタマイズ等が発生した場合に実施するシステムの構成変更作業等
	システム外要因	電源、外部接続回線等システム外要因の計画停止に伴う停止

10. 稼動監視

（1）概要

監視とは、常にシステムの稼動状況を動的に把握することである。具体的には、システムに接続されている機器やサービスの稼動状況、システムパフォーマンス（システムリソース）等、動的な情報を収集し確認する。

（2）監視対象

ア　当事業広報啓発 WEB サイト

イ　e ラーニングシステム

（3）監視内容

システムの正常稼働を、以下の項目において監視すること。

項目	内容	周期
システム死活監視	定期的に Ping コマンドを実行し、監視対象となる機器の死活を監視する	随時
サービス監視	サービスの TCP ポートとプロセスが正常に稼働しているかを監視する また、HTTP、FTP、CMS、MySPL などの各種サービスの稼働を監視する	随時
CPU 監視	CPU の使用率を監視し、定めた閾値になるとアラームを発し事前通知する	随時
ディスク監視	ディスクの使用率を監視し、定めた閾値になるとアラームを発し事前通知する	随時
メモリ監視	メモリの使用率を監視し、定めた閾値になるとアラームを発し事前通知する	随時
トラフィック監視	対象の機器のパケット状況を監視し、正常値を超えた場合アラームを発する	随時
パフォーマンス監視	公開されているページの異常（バグやリンク切れなど）を検知し異常を発する	随時

ファイアウォール監視	データベースをはじめとするサービスサーバへの不正アクセス及び過剰アクセスを監視する	随時

（4）異常検知方法

特定の閾値に達した場合、警報（音声・ランプ点灯）をデータセンター職員に向けて発報し事前復旧を行う。また、関係者へも通知メールを配信し、異常検知を迅速化する。

11. 保守サポート対応

（1）概要

公開後の軽微な改修に関する要望に対し、予め設定する保守サポート作業時間内において修正またはサポート対応する。

（2）保守サポート作業時間

月間 5 時間以上を標準とする

（3）保守サポート管理方法

システム課題等が委託者および利用者から指摘された場合は、対応項目を管理し委託者と対応方法を協議の上、保守サポート作業時間内にて対応する。

以上