

甲府市行政情報システム更改・運用業務 サービス要件書

サービス要件書		サービス仕様	サービス仕様の補足
1.事業・サービス運営			
1.1 情報共有・協議			
1.1.1 情報共有・協議	本市、事業者内部及び関係者との連絡・調整、情報共有及び協議を適切に実施し、契約・仕様上必要な報告、協議及びエスカレーションを確実に履行すること。	本市の情報政策担当部署及び業務担当部署、事業者内部の各関係部署並びにその他の関係者と十分なコミュニケーションを図ること。特に、重大な課題、懸念事項又はサービス影響が見込まれる事項については、把握後速やかに本市へ共有すること。通常時及び緊急時の連絡・エスカレーション条件は、別紙モニタリング基準又は運用関連文書に定める。本項は契約・仕様上の履行状況を確認する項目として扱う。	
1.2 継続的改善			
1.2.1 事業に対するサービスの継続的改善	サービス品質及び運用効率の継続的な改善に取り組むこと。サービス提供上の課題、懸念事項及び改善余地を主体的に把握するとともに定期的に調査を行い、改善が必要な事項については、原因及び課題を分析の上、改善内容、期待効果及び実施時期を整理して本市へ提案すること。	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。	
1.2.2 事業者内部の業務改善	随時、自主的な業務改善に取り組み、報告すること。	レビュー品質向上、リスク分析向上に取り組み、改善状況を定期的に報告すること。 品質改善活動をレビューする事業者内フローを整備し運用すること。	
1.3 コンプライアンス／法令・制度対応			
1.3.1 法令・制度改正への対応	受注者は、開発期間中に公表・施行される関連法令及び制度改正等について継続的に情報収集し、当該システムへの影響を調査・評価し、本市と協議の上、対応の要否を含む対応方針を決定し、必要な設計・実装への反映を適切に行うこと。	他団体の事例を踏まえ、条例・規則等の変更も含め、業務の効率的な実施手法についての提案を行うこと。	
1.4 サービスレベル管理			
1.4.1 モニタリング・サービスレビュー	事業全般の年間計画を策定し、目標管理を行うこと。 月次・四半期・年次で実績報告を行うこと。事業者はセルフモニタリング実施計画書に基づき、契約期間中、毎月サービス品質の充足状況を確認し、翌月に報告書を提出すること。	本事業の収支を独自に管理し、毎年度収支報告を行うこと。具体的な手法や報告書の内容等については、本市と協議し、プロジェクト計画書に記載すること。 提出期限の管理、未提出時の督促等の運用については、モニタリング報告書による実施状況の確認とあわせて定めること。	
1.4.2 収支管理	本事業の収支を管理し、報告すること。	本事業の収支を独自に管理し、毎年度収支報告を行うこと。具体的な手法や報告書の内容等については、本市と協議し、プロジェクト計画書に記載すること。 提出期限の管理、未提出時の督促等の運用については、モニタリング報告書による実施状況の確認とあわせて定めること。	
1.5 事業継続・引継ぎ			
1.5.1 事業完了時・破綻時のサービス継続、次期事業者への引継ぎ	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。契約終了に際しては、サービスの継続及び次期事業者への移行に必要な情報・資料を最新の状態で提出し、円滑な引継ぎを支援すること。	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。次期事業者への引継ぎ完了まで、従前のSLA水準を維持して運営を継続すること。秘密情報は、本市の指示に従い消去し、その実施結果を報告すること。	
2 サービス提供・品質			
2.1 サービス提供時間・可用性			
2.1.1 稼働時間・業務時間	事業関連図書で特に指定する場合を除き、稼働時間は、土曜日と祝祭日、および12月30日から1月3日を除く全ての日で原則7:30～24:00とする。また、業務時間は、同期間を除く全ての日について、原則として8:30から17:15までとする。 ただし、本市と事業者が事前に協議の上、これらの時間以外に稼働する場合は、当該時間を稼働時間を含むものとする。	稼働時間・業務時間については、事業者の提案により延長する場合もある。	
2.1.2 計画停止	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、年間総稼働時間の1%以下であること。また、一回の停止時間については、本市の承認を得て決定すること。	稼働時間内に、職員もしくは市民の利用に何らかの影響のある機能等が計画的にかつ正常に使用できない場合を、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本市の承認を得ること。	
2.1.3 予定外停止	予定外のシステム停止時間の総計は、総稼働時間の0.5%以下であること。	稼働時間内に、職員もしくは市民の利用に何らかの影響のある機能等が予定されずにかつ正常に使用できない場合を、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・キャパシティ			
2.2.1 常時の性能維持	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。	業務仕様書等に個別の定めがある場合を除き、通常時3秒以内、アクセス集中時5秒以内を基本目標とする。帳票出力については、印刷指示から印刷開始まで10秒以内を基本目標とする。対象処理、測定条件、測定頻度及び測定方法は、別紙モニタリング基準に定める。	
2.2.2 性能維持に必要な諸条件	運営管理期間中、システムの利用状況、処理量及びリソース使用状況等を継続的に把握し、サービス品質に影響する性能低下が見込まれる場合は、必要な対策を事前に実施すること。	性能低下の兆候を継続的に確認し、性能低下又はその可能性を把握した場合は、原因及び影響範囲を分析し、設定変更、リソース増強その他必要な対応を行うこと。また、システム変更、バージョンアップ等を行う場合は、必要に応じて性能への影響を事前に確認すること。	
2.2.3 ハードウェア容量・必要性能の予測、確保	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。 なお、ハードウェア等の資産を本市は原則保有せず、また、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。	
2.2.4 繁忙期・ピーク時の性能維持	受注者は、繁忙期その他アクセスが集中する時期においても、業務実施に支障を及ぼさない性能を維持すること。この場合の性能の判定は、補足に定める測定条件に基づいて行うものとし、利用者端末環境に起因する性能低下を含まない。	業務仕様書等に個別の定めがある場合を除き、アクセス集中時のオンラインレスポンスタイムは5秒以内とする。 ※「アクセス集中時」とは、年度末、月末、申請期限直前等、アクセスが特に集中する期間及び時間帯をいう。対象となる処理は、業務仕様書に定めるオンライン処理のうち、本市が指定するものとする。 オンラインレスポンスタイムは、本システムの標準稼働環境(利用者端末のスペック、ネットワーク環境を含む。))において測定した値とし、標準稼働環境を満たさない利用者端末に起因する性能低下は、本項の性能要件の不達とはみなさない。標準稼働環境の具体的な構成は、業務仕様書に定める。 また、性能低下の報告を受けた場合は、受注者は、本システムに起因するものであるか否かの切り分けに必要な調査(システム側の状況確認、ログの確認等)を行い、その結果を本市に報告すること。切り分けの結果、利用者端末環境又は本システム以外の要因によることが判明した場合は、その内容を含めて報告し、本市が端末管理者等への対応を判断できるようにすること。 測定は、システム構築時の負荷試験及び運用時の定期監視により行うものとする。	
2.2.5 パッチ・ジョブ処理性能	業務上重要なパッチ処理及びジョブについて、後続処理及び業務開始に支障を及ぼさない時間内に処理を完了すること。また、異常終了等が発生した場合に必要な再実行又は復旧を行うための時間を確保すること。	重要なパッチ処理及びジョブについて、処理対象、処理量、実行時間帯、後続処理、業務開始時刻等を踏まえて、処理完了の目標時刻又は許容時間を設定すること。 目標時刻又は許容時間は、異常終了その他の問題が発生した場合に、再実行、復旧その他必要な対応を実施するための時間を確保できるよう設定すること。 処理時間の実績及び傾向を継続的に確認し、処理時間の長期化又は業務影響のおそれを把握した場合は、原因を分析し、必要な改善を行うこと。	
2.3 システム運営・保守			
2.3.1 システム運営・保守	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、正常な稼働を保証すること。 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。	
2.4 サポートサービス			
2.4.1 サポートデスク	サポートデスクを安定的に運営し、利用者からの問い合わせに対する受付・応答・解決品質を維持すること。	サポートデスクでは、業務処理の先例・他団体の処理事例についての問い合わせにも対応すること。 業務仕様書に個別の記載がある場合を除き、サポートデスクの正常な稼働は、以下の指標を基準とする。 稼働率:業務時間の95%以上 途中放棄率:全コールの5%以下 一次完結率:全コールの80%以上	
2.5 障害対応・運用監視			
2.5.1 障害発生時の初報	業務や市民サービスに影響を与える障害は、発生から10分以内に本市へ通知し、早急に復旧させること。	障害のタイプ別に検知手法を用意し、本市のレビューを受けること。 障害の検知・通知方法及び復旧手法を、障害のタイプ別に明示すること。	
2.5.2 影響範囲特定・復旧予定時間の報告	業務や市民サービスに影響を与える障害が発生した場合は、発生又は検知後30分以内に、判明している影響範囲及び初動対応の状況を本市に報告すること。また、発生又は検知後2時間以内に、詳細な影響範囲、復旧方針及び復旧予定時刻を報告すること。	業務や市民サービスに影響を与える障害が発生した場合は、発生又は検知後30分以内に、判明している影響範囲及び初動対応の状況を本市に報告すること。また、発生又は検知後2時間以内に、詳細な影響範囲、復旧方針及び復旧予定時刻を確定することを目標とする。 障害調査プロセスや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。 業務時間内においては、本市からの電話連絡を常に受け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。	
2.5.3 サービス稼働監視・ログ管理	問題の予兆及び発生を早期に検知できるよう、各種サービスの稼働状態を継続的に監視するとともに、障害対応及び原因分析に必要なログを取得し、適切に保管及び管理すること。	ハードウェアの稼働状態に加え、ソフトウェア及びサービスを構成する各プロセスの稼働状態並びにリソースの使用状況を監視し、異常を即時に検知できること。取得するログの種類、取得方法及び保存期間等のログ採取方針並びに分析方法を明示し、ログの改ざん及び不正な削除を防止するための措置を講じること。また、障害発生時には必要なログを速やかに調査・分析し、その結果を本市に報告するとともに、本市の求めに応じてログを提出できる状態とすること。なお、個人情報その他の機密情報を含むログについては、適切なアクセス制御を実施すること。	
2.5.4 監視基準・監視レベル管理	サービスの重要度及び障害影響を踏まえ、監視対象、監視間隔、警戒閾値及びアラート基準を設定し、サービスレベル低下の兆候を早期に検知できる監視レベルを維持すること。	具体的な監視対象、監視間隔、警戒閾値、アラート条件及び通知条件は、別紙モニタリング基準に定める。	
2.6 セキュリティサービス			
2.6.1 セキュリティ防御・運用	システム及びサービスに対する不正アクセス、不正利用その他のセキュリティ上の脅威を継続的に監視し、必要な防御、検知及び対応を実施すること。また、脅威、利用状況及びシステム構成等の変化を踏まえ、セキュリティ対策を定期的に確認・見直し、安全なサービス提供を維持すること。	認証及びアクセス権限を適切に管理し、不正アクセス、不審な認証その他の異常を把握できるよう必要なログ及び記録を取得・保管し、継続的又は定期的に確認すること。重要なデータの参照、更新、出力、移動等について必要な操作記録を確認できる状態を維持すること。セキュリティ対策は単一の防御手段に依存せず、認証・認可、アクセス制御、ログ監視、マルウェア対策その他の必要な対策を組み合わせて、その有効性を定期的に確認・見直すこと。	
2.6.2 セキュリティホール・脆弱性対応	システム及びサービスに影響を及ぼすセキュリティホール、脆弱性その他のセキュリティ上の問題を継続的に把握し、その影響及び緊急度を評価した上で、必要な対策を適切な時期に実施すること。	OS、ミドルウェア、アプリケーションその他システムを構成するソフトウェア等について、脆弱性情報及びセキュリティ関連情報を継続的に収集・確認すること。脆弱性等を把握した場合は、システムへの影響、重要度、悪用の有無・可能性等を踏まえて対応の優先度を判断し、必要に応じて本市へ報告するとともに、パッチ適用、設定変更、アクセス制限その他の暫定対策又は恒久対策を実施すること。対策実施時はサービスへの影響を確認し、必要に応じて事前検証を行うこと。	

甲府市行政情報システム更改・運用業務 サービス要件書

サービス要件書		サービス仕様	サービス仕様の補足
	2.7 災害時サービス継続・復旧		
	2.7.1 災害時のサービス継続・復旧	災害時におけるサービス継続を確保するため、事業継続計画を策定・実施するとともに、当該計画について常に最新の状態を維持すること。事業継続計画の実施内容については、継続的に確認・検証を行い、その結果を本市に報告すること。また、大規模災害により本システムが損壊した場合を想定し、発生時から①1週間以内、②1か月以内、③1か月以降の各フェーズにおけるサービス提供方法を策定すること。	本事業の期間中を通じて、事業者、構成企業又は製品提供元の破綻等、事業又はサービスの継続に支障を来す事象を想定し、具体的な対応方法を定めること。 事業継続計画の策定及び通常想定される対策は、原則として本事業の範囲内とすること。 大規模災害発生時には、フェーズ①(発生時から1週間以内)及びフェーズ②(1か月以内)に係る復旧対策の検討・準備を本事業の範囲内とすること。フェーズ③(1か月以降)については、災害発生前と同等の業務レベルを維持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。 継続的な確認・検証は、事業継続計画に基づく訓練又はレビューの定期的な実施により行い、その結果を本市に報告すること。 想定を超える激甚災害その他の不可抗力により、通常の事業継続対策の範囲を超える対応が必要となる場合は、本市と事業者が協議の上、対応内容及び費用負担を決定すること。
	2.8 バックアップ・復旧		
	2.8.1 バックアップ管理	業務継続及びシステム復旧に必要なデータ等について、定めた条件に基づきバックアップを取得・保管し、取得結果を継続的に確認すること。	バックアップ対象、取得間隔、保存期間等を定め、RPO及び保存要件等と整合するようバックアップを実施すること。取得失敗又は異常を検知した場合は、速やかに再取得その他必要な対応を実施すること。
	2.8.2 復元確認・リストア試験	取得したバックアップについて、所定の復旧手順により復元可能であることを定期的に確認すること。確認の結果、不備が認められた場合は必要な改善を行うこと。	復元確認の対象、方法、頻度及び判定基準を業務・システムの重要度を踏まえて定めること。重要業務については年1回以上を基本として復元確認を実施し、復元可否及び所要時間を確認すること。不備を確認した場合は、原因を分析し、必要な是正及び再確認を行うこと。
3. マネジメント			
3.1 基本事項			
	3.1.1 PMBOKを踏まえたマネジメント	一般的な標準(PMBOK)に基づくプロジェクトマネジメント及びリスクマネジメントを行い、品質を適切に管理するとともに、本市及び関係者との円滑なコミュニケーションを行うこと。 また、事業者内部を含むプロジェクトマネジメントの状況、課題、対応状況及び重要な協議・合意事項について記録・管理し、本市が必要に応じて確認できる状態を維持すること。	プロジェクト管理に必要な計画書、報告書その他の資料を適切に作成・管理すること。 課題、リスク、タスク、協議・合意事項等について、経緯及び対応状況を追跡できるよう記録・管理し、本市及び関係者が必要な情報を共有・確認できる環境を整備すること。 具体的な管理手法及び使用するツールについては、本市と協議の上決定すること。
	3.1.2 プロジェクトに必要な体制・要員管理	プロジェクトに必要なリソースは、本市分も含めて把握・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。また、設計・構築・運用、セキュリティ、コスト管理等に必要な知識・経験を有する要員を配置し、継続的に最適化できる体制とすること。	本市が行うべき作業、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。
	3.1.3 重要ドキュメントの整備・最新化・履歴管理	プロジェクト計画書、要件定義書、システム設計書、データ構造設計書、テスト計画書、移行計画書、運用計画書、障害対応計画書、事業継続計画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。	既存の文書によって合意された内容や要件と異なる場合には、文書により承認を取り、変更を実施すること。 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。
	3.1.4 ナレッジ・引継ぎ管理	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。	特にプロジェクトマネージャー等、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品質が低下する例が多いため、単純な引継ぎの充実に以外に、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こと。
3.2 進捗管理			
	3.2.1 マイルストーン・作業計画の管理	受注者は、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したWBS(作業分解構造)による管理を行うこと。この場合の作業単位は、進捗の把握及び報告に足る粒度とすること。	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。フェーズ又はタスク毎の完了基準を明確にすること。 WBSの作業単位は、原則として作業期間が2週間以内となる粒度に分解すること。作業期間が2週間を超える作業については、中間成果物又は中間確認点を設定し、当該作業の進捗を確認できるようにすること。ただし、長時間を要する負荷試験、外部調達に係る待ち時間等、作業の性質上、分解することが不適切な作業については、この限りでない。この場合においては、進捗を確認するための代替の方法を本市と協議の上、定めること。
	3.2.2 進捗管理・工数管理	作業計画に基づき、各作業の予定及び実績並びに投入工数を継続的に把握し、進捗状況を管理すること。 遅延又は工数超過のおそれを把握した場合は、プロジェクト全体への影響を分析し、必要な対応を講じるとともに、本市に報告すること。	各作業の予定日、実績日、予定工数及び実績工数を管理し、後続作業及び要員計画への影響を確認すること。また、遅延又は工数超過が見込まれる場合は、その原因、影響、対応策及び解消見込みを本市に報告すること。
3.3 品質管理・品質保証			
	3.3.1 品質管理(記録・分析・改善)	品質の管理は、可能な限り体系的に記録し、発生箇所・頻度・原因等の分析管理を行い品質向上に継続して取り組むこと。	プログラム開発の品質管理指標だけではなく、業務パッケージに関する指標も分析管理し報告すること。 また、仕様ミス・デプロイミス・テストシナリオ不足など、SIサービス等に関連した品質管理指標についても分析管理し報告すること。
	3.3.2 品質保証(レビュー・検査)	プログラムやドキュメント等の成果物については、体系的に管理するとともに、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リスク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・更新を行うこと。 レビューが行われていること、レビュー観点が有効であること、影響分析・リスク分析が適切であることを確認する方法を確立し、必要に応じ本市に報告できるようにしておくこと。 バージョン管理、バグトラッキング、継続的インテグレーション、構成管理等のDevOpsツールや手法を導入し、開発や運用を効率化させること。
3.4 リスク・課題管理			
	3.4.1 リスク・課題の識別・評価	プロジェクトに関する課題・リスクを常に漏れなく管理し、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。	リスク管理表を整備し、本市と常に共有すると共に、プロジェクト全メンバーが適切に認識するようマネジメントを行うこと。また、必要な場合は本市へも前もってリスク対策を要求すること。 リスク管理表においては、機能・帳票のカスタマイズ、計算処理、連携処理、移行データなどリスクの発生しやすいポイントが整理され、リスクの発生箇所や原因別に分類し管理を行うこと。
	3.4.2 リスク対応	プロジェクトに関するリスクを低減できるよう、常に検討を行い、対策を提案すること。	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)を設けること。 リスク管理やリスク対策が適切に行われずにリスクが顕在化した場合は、事業者の責任と負担においてサービス品質の維持を行うこと。
	3.4.3 独立レビュー・監査対応	リスク分析及びリスク対策を、第三者的に検証する仕組みを備えること。	人的ミス、システム障害、SIサービスの品質劣化、セキュリティ事故等のリスクシナリオについて詳細化・整備を常に行い、有識者等によるレビューを受けること。 本市側が監査を行う場合は対応できること。
3.5 要件・変更管理			
	3.5.1 要件充足状況の管理	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、もしくは本市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を。	業務要件の充足度を確認・検討する手法を提供すること。
	3.5.2 システム変更等を行う際の影響・適合確認	システムに採用する製品、プログラム、構成、設定その他の仕様を変更する場合は、変更内容、変更理由、影響範囲、実施方法及び切戻し方法を明確にし、事前に本市の承認を得ること。また、変更の実施結果を確認し、その履歴を管理すること。	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本市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。
3.6 テスト管理			
	3.6.1 テスト	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。 テスト対象のインストール内容を基に影響範囲を分析し、分析結果に基づいたテストシナリオを構築し、有識者のレビューを受けること。 バッチ処理結果等、業務データのテスト結果について本市側でチェックを行う手法・ツールを提供すること。
3.7 データ移行・切替管理			
	3.7.1 データ移行・切替管理	業務に必要なデータを既存システムから次期システムへ確実に移行するとともに、移行前後のデータ件数及び内容を照合し、移行結果の完全性及び正確性を確認すること。また、移行リハーサル、エラー発生時の対応及び切戻し手順を定め、本市の承認を得たうえで本番移行及び切替えを実施すること。	データ移行作業は原則として事業者で実施すること。
3.8 ライフサイクル管理			
	3.8.1 EOL/EOS管理	受注者は、本システムを構成するハードウェア、ソフトウェア(OS、ミドルウェア、データベース管理システム等)及びその他の調達製品について、製造元・ベンダーが公表するサポート終了(EOS)・販売終了(EOL)等のライフサイクル情報を継続的に収集・管理すること。この場合において、サポート終了等に起因するリスク(セキュリティ修正の提供終了等)が生じないよう、あらかじめ本市と協議の上、計画的な更新・移行等の対応を行うこと。	ライフサイクル管理の対象製品一覧及び各製品のサポート終了時期を整理した管理台帳を作成・維持し、少なくとも年1回見直しを行い、その結果を本市に報告すること。サポート終了が予定されている製品を把握した場合は、その影響(セキュリティリスク、他システムへの影響等)を評価し、更新時期及び移行計画を盛り込んだ対応方針を、サポート終了前に本市へ提案すること。また、サポート終了後も継続使用が必要となる場合は、リスク低減策(ネットワーク分離、脆弱性対策の代替措置等)を本市と協議の上、実施すること。
3.9 情報セキュリティ管理			
	3.9.1 事業者の作業実施時の情報流出防止	システムに関する作業を実施する場合は、情報の漏えい、紛失、改ざん、不正利用等を防止するため、作業内容及び取り扱う情報の重要度に応じた安全管理措置を講じること。	情報へのアクセス、データの出力、持出し、複製及び運搬について、作業者、作業内容及び取扱状況を記録し、確認できる状態とすること。データを外部へ持ち出し、又は運搬する必要がある場合は、事前に本市の承認を得たうえで、暗号化その他の安全管理措置を講じること。作業完了後は、持ち出したデータ及びその複製物を確実に返却又は削除し、その結果を本市に報告すること。