仕様書

1　件名

令和８年度　生活保護システムの提供等業務

2　目的

生活保護業務の効率的な執行を行うため、被保護者台帳の整備、支給保護費の算出及び支給処理等を一体的に管理する電算システムの運用を行うことを目的とする。

3　利用場所

岩沼市桜一丁目 6 番 20 号外　地内

4　利用期間

令和８年４日１日から令和９年３月３１日まで

5　サービス利用範囲

（1）標準準拠アプリ（ガバメントクラウドサービス提供基盤のCSPは、AWSの共同利用環境とする）

システム名称	システム構成
生活保護システム （標準実装）	・基本業務(標準仕様書第 1.1 版による） ・返還金（債権管理） ・他法活用支援 ・受診指導支援 ・自立就労支援 ・番号制度連携 ・オンライン資格連携

（2）クライアントライセンス

生活保護システムクライアントライセンス数（上限）	１０台

（3）アプリケーション保守・システム運用支援・運用管理補助

クラウド利用サービスに含まれるサービス内容は別紙１に記載

（4）非機能要件の基準

クラウド利用サービスに含まれるサービス内容は別紙２に記載

（5）データ消去について

利用期間中にサービス利用が終了となる際は、データ消去を実施する。ただし、サービス利用終了時点の「地方公共団体における情報セキュリティポリシーに関するガイドライン」を考慮し、協議の上実施方法を決定する。

6　利用料の支払い

利用料は毎月払いとする。賃借人は賃貸人からの請求書受理後、30 日以内に支払う。

7　その他

本仕様書に定めのない事項について疑義が生じたときは、賃貸人と賃借人が協議し決定するものとする。

（別紙１）
１．アプリケーション保守・システム運用支援・運用管理補助

項目	内容
アプリケーション保守	①　標準版アプリケーション保守 ・標準版アプリケーションのパッチ適用及びバージョンアップ ※UI 等機能改善含む ・パッケージソフトウェアのバージョンアップ計画やマイグレーション計画の策定等 ・パッケージソフトウェアを利用したシステムのサイジング（システム基盤は AWS）を実施し、最適化を実現 ・パッケージソフトウェアのライブラリや他システムとの連携を考慮した保守や改修 ②　生活保護標準仕様書の改版に伴う標準準拠版機能の対応 ・年度単位で更新される標準仕様書の改版の機能追加対応を含むものとする。 ※他標準準拠システムのデータ・連携要件に関する対応は原則含まないこととし、機能追加可否の判断は受注者判断に依ることとする ③　法・制度改正に伴うシステム改修対応 ・法制度の新設あるいは改正・制度変更に伴う、システム機能の追加・改修 ※国庫補助金・交付金等が支給される改正及び新制度等の対応は除く
システム運用支援	①　サポートデスク運営・維持 ・コールセンター（ヘルプデスクによるサポート）対応 ・お客様サポートサイトによる情報提供 ・マニュアル改訂 ②　障害対応 ・障害箇所の復旧、報告、インシデント管理 ・リモートでのデータ調査及び復旧または復旧方法の説明 ※発注者の障害（ウィルス感染等）に起因する復旧作業は除く
運用管理補助	ガバメントクラウド（生活保護業務共同利用領域のみ）の運用管理補助者対応 ①　クラウドインフラの設計（権限管理含む)、構築、運用、保守、継続的な改善 ②　ガバメントクラウド共同領域の利用権限管理 ③　クラウドサービス等を利用し、運用管理する際の技術的助言、補助等 ④　ネットワーク管理補助者及びアプリケーション提供事業者との間で、当該アプリケーション等の利用のための必要な連絡 ⑤　共同利用領域の WSUS およびウィルス対策ソフトの対応 ⑥　データ連携状況確認及び共同利用領域の監視アラート発生状況をまとめ、四半期ごとに遂行状況等をオンラインで資料提供 ⑦　デジタル庁に支払うクラウドサービス等利用料の集計・複数の地方公共団体間での按分等の調整 ※支払い代行業務は範囲外とする

次項に続く

２．稼働等要件（ＳＬＡ）

No	設定項目		設定値	備考
1	可用性	システム稼働時間	07：00～22：00	ただし、定期保守やデータバックアップ等のシステムの維持管理に必要となる計画停止は除く ※設定値の時間帯は、双方合意により個別設定する場合がある
		ヘルプデスク対応時間	09：00～12：00 13：00～17：00	土日、休日、年末年始（各年度で休業日を決定）は除く
		バックアップ	日次	１営業日前を最新として 7 世代分のバックアップを保持
		稼働率	99.5%以上	サービスに影響のない一部機能のみの停止を除く ※システム稼働時間が上記と異なる場合は、双方合意した稼働時間に基づき稼働率を算定する ※通信障害によるシステム停止時間を除く ※ウィルス感染等、発注者側の障害起因によるシステム停止時間を除く ※システムメンテナンス時間を除く
2	性能	オンライン応答時間（通常時）	平均 3 秒以内	推奨環境で利用する場合
		オンライン応答時間（アクセス集中時）	平均 5 秒以内	推奨環境で利用する場合
3	信頼性	一次通知（障害検知）	1 時間以内	
		二次通知（対応検知）	2 時間以内	
		リカバリポイント	前回バックアップデータ	

なお、この要件は努力目標とするが、要件を遵守出来ずに業務遂行に著しい影響を与えた場合は双方協議の上、適切な対応策を講じるものとする。

３．サービスメンテナンス

（1）メンテナンス作業

安定したクラウドサービスをご提供するため、メンテナンス作業を以下のとおり実施する。

1	通常メンテナンス（定期）	実施日	プログラム更新等を前提に、月に 1 回定期メンテナンスを実施する。 実施日及び作業時間については双方協議のうえ決定する。
		通知日	適用 1 週間前までに、メール等により通知を行う。 ※緊急時は別途対応とする
2	緊急メンテナンス	通知日	原則、作業実施前のメール等により通知を行う。

（2）サポート窓口

1	電話窓口	営業時間内においては、電話窓口において照会に応じる体制を確保する。
2	電子メール	電子メールによる照会に応じる体制を確保する。なお、営業時間外の照会についての回答は翌営業日以降とする。

（別紙２）

非機能要件については、「地方公共団体情報システム非機能要件の標準_生活保護_第 1.1」各要求に対し、以下選択レベルを基準とする。

■全庁的要求事項

項番	大項目	中項目	選択レベル		レベル								サービス提供選択レベル	共同利用方式の環境における選択レベル概要
					-	*	0	1	2	3	4	5		
C.1.2.2	運用・保守性	通常運用	2	システムの復旧に外部データを利用できない	仕様の対象としない	ベンダーによる提案事項	外部データによりシステムの全データが復旧可能	外部データによりシステムの一部のデータが復旧可能	システムの復旧に外部データを利用できない				2	システムの障害時等においては、外部データを利用せずCSP内（別リージョン）に保存したバックアップファイルのみから復旧対応とする。
C.2.3.5	運用・保守性	保守運用	4	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	仕様の対象としない	ベンダーによる提案事項	パッチを適用しない	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	緊急性の高いパッチのみ即時に適用し、それ以外は障害対応時等適切なタイミングで適用を行う	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行う	新規のパッチがリリースされるたびに適用を行う	4	緊急性の高いパッチについては、サービス提供側にて該当する脅威が提供システムやセキュリティへの影響を判断し、社内検証実施後に速やかにパッチ適用を行う。 その他パッチについても社内検証を実施し、定期保守等のタイミングでの適用を実施する。 ※予定
E.1.1.1	セキュリティ	前提条件・制約条件	1	有り	仕様の対象としない	ベンダーによる提案事項	無し	有り					1	ガバメントクラウド上に構築する標準準拠システムについては、以下を遵守することを前提として提供する。 ・情報セキュリティに関する法令 ・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）
E.2.1.1	セキュリティ	セキュリティリスク分析	1	重要度が高い資産を扱う範囲	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲	対象全体				1	重要度が高い資産は、各団体の情報セキュリティポリシーにおける重要度等に基づいて定める内容に沿った対応とする。
E.4.3.4	セキュリティ	セキュリティリスク管理	2	定義ファイルリリース時に実施	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				2	サービス提供側の運用管理環境から生活保護システム本番サーバに対して、適宜定義ファイルの更新を実施する。
E.5.1.1	セキュリティ	アクセス・利用制限	3	複数回、異なる方式による認証	仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			3	標準準拠システムの管理権限を持つ主体の認証は、自治体様が求める二要素認証等に合わせた対応とする。 （二要素認証を実施する場合の管理は、自治体様の対応とする。）
E.5.2.1	セキュリティ	アクセス・利用制限	1	必要最小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のみ許可する。	仕様の対象としない	ベンダーによる提案事項	無し	必要最小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のみ許可する。					1	標準準拠システムの利用以外では、サーバなどにはアクセスをさせない環境にて提供を行う。 各種ファイル・データへのアクセスについては、システムからのアクセスのみを許可し、不要なアクセス方法を制限する。
E.6.1.1	セキュリティ	データの秘匿	3	すべてのデータを暗号化	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			3	生活保護システムにて使用する伝送データは、以下の方式で暗号化を実施する。 ①通常通信方式　　：httpsによる暗号化 ②データ連携通信　　：標準仕様書(連携要件)に沿って暗号化 ③データベースの暗号化：RDSの暗号化機能を利用 なお、標準化対象外の外部機関との連携通信や同システム内の通信においては、相手先の連携仕様に従うため、暗号化の対象外となる。
E.6.1.2	セキュリティ	データの秘匿	3	すべてのデータを暗号化	仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			3	標準準拠システムで使用するデータベースやオブジェクトストレージおよびデータ保管されるサービスについては、全て暗号化を実施する。
E.7.1.1	セキュリティ	不正追跡・監視	1	必要なログを取得する	仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					1	CSPのマネージドサービスを利用して、必要なログを取得する。 （アプリケーションログ・ミドルウェアログ・データ連携ログ・通信ログ等）
E.7.1.3	セキュリティ	不正追跡・監視	1	重要度が高い資産を扱う範囲	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲	システム全体				1	E.7.1.1と同様
E.10.1.1	セキュリティ	Web対策	1	対策の強化	仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					0	インターネットに接続したWebアプリケーションを用いないため、対策強化は無しとなる。
E.10.1.2	セキュリティ	Web対策	0	無し	仕様の対象としない	ベンダーによる提案事項	無し	有り					0	内部ネットワークのみ接続する情報システムのためWAFの導入は不要とし、対象外とする。

■業務主管部門要求事項

項番	大項目	中項目	選択レベル		レベル								サービス提供選択レベル	共同利用方式の環境における選択レベル概要
					-	*	0	1	2	3	4	5		
A.1.3.1	可用性	継続性	2	1営業日前の時点（日次バックアップからの復旧）	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ、一時保存データからの復旧）			2	業務停止となる障害が発生しデータの消失等が発生した場合には、日々のバックアップデータより復旧を実施する。 （バックアップについては、１営業日前を最新として7世代分のバックアップを保持） ※大規模災害において、CSPへの影響があるような障害の場合、項番A.1.4.1記載の内容となる。
A.1.3.2	可用性	継続性	2	12時間以内	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		2	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際には、起動テンプレートおよびバックアップデータからの復旧を実施する。 上記の作業にかかる対応として、12時間以内での対応を予定。 （共同利用環境において、サービス提供側のセキュリティルームからの保守が可能であることが前提となる。） ※ハードウェア・ミドルウェアの対象として、サービス提供側が提供するガバメントクラウド上にある環境のみを対象とする。 ※庁内のネットワークや電源設備などによる障害は対象外となる。 ※大規模災害において CSPへの影響があるような障害の場合、項番A.1.4.1記載の内容となる。
A.1.3.3	可用性	継続性	2	全システム機能の復旧	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				2	業務停止を伴う障害が発生した際の対応としては、サービス提供側システムの機能すべてを対象とする。 共通機能（データ連携等）については、連携先システムの状況に依存するため、別途対応が必要となる場合がある。 ※ハードウェア・ミドルウェアの対象として、サービス提供側が提供するガバメントクラウド上にある環境のみを対象とする。 ※庁内のネットワークや電源設備などによる障害は対象外となる。 ※大規模災害において CSPへの影響があるような障害の場合、項番A.1.4.1記載の内容となる。
A.1.4.1	可用性	継続性	2	一ヶ月以内に再開	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	2	大規模災害の規模に応じては、CSPの別リージョンへの構築とするかなどの協議が必要となる。 （バックアップファイルについては、別リージョンへのマルチバックアップを予定している。） 災害規模に応じては、システム構築以外の被災地の復旧拠点に応じて対応が異なることが予想される。 サービス提供側および庁内のネットワークや電源設備などが復旧していることを前提として、一ヶ月以内での対応とする。 共通機能（データ連携等）については、連携先システムの状況に依存するため、別途対応が必要となる場合がある。
A.1.5.1	可用性	継続性	3	99.5%	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	3	99.5%・・・・・年間の累計停止時間は14.5時間でのサービス提供を予定している。 ※システムのオンライン提供時間により、停止時間は変更となる。 ※システムメンテナンス時間は、対象外となる。
B.1.1.1	性能・拡張性	業務処理量	1	上限が決まっている	仕様の対象としない	ベンダーによる提案事項	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				1	自治体毎に予めヒアリングや現行データ内容を換算し、環境構築・システムパラメータの設定を実施する。
B.1.1.2	性能・拡張性	業務処理量	1	同時アクセスの上限が決まっている	仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り				1	自治体様毎に予めヒアリングや現行データ内容を換算し、環境構築・システムパラメータの設定を実施する。
B.1.1.3	性能・拡張性	業務処理量	0	すべてのデータ件数、データ量が明確である	仕様の対象としない	ベンダーによる提案事項	すべてのデータ件数、データ量が明確である	主要なデータ件数、データ量のみが明確である					0	自治体様毎に予めヒアリングや現行データ内容を換算し、環境構築・システムパラメータの設定を実施する。
B.1.1.4	性能・拡張性	業務処理量	0	処理ごとにリクエスト件数が明確である	仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である					0	自治体様毎に予めヒアリングや現行データ内容を換算し、環境構築・システムパラメータの設定を実施する。
B.1.1.5	性能・拡張性	業務処理量	0	処理単位ごとに処理件数が決まっている	仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					0	自治体様毎に予めヒアリングや現行データ内容を換算し、環境構築・システムパラメータの設定を実施する。
B.2.1.4	性能・拡張性	性能目標値	3	3秒以内	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		3	ガバメントクラウドに構築した標準準拠システムにおいて、通常時のオンラインレスポンスは主要機能におけるレスポンスを３秒以内を実現する。 ※月次・年次処理や大量印刷は上記記載の時間を超える場合がある。 ※個人を特定した処理を実施する画面を主要機能とする。 ※サービス提供側の推奨スペックでの提案が不可の場合については、協議させていただく場合がある。
B.2.1.5	性能・拡張性	性能目標値	2	5秒以内	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		2	ガバメントクラウドに構築した標準準拠システムにおいて、通常時のオンラインレスポンスは主要機能におけるレスポンスを５秒以内を実現する。 ※月次・年次処理や大量印刷は上記記載の時間を超える場合がある。 ※個人を特定した処理を実施する画面を主要機能とする。 ※サービス提供側の推奨スペックでの提案が不可の場合については、協議させていただく場合がある。
B.2.2.1	性能・拡張性	性能目標値	2	再実行の余裕が確保できる	仕様の対象としない	ベンダーによる提案事項	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				2	ガバメントクラウドに構築した標準準拠システムのバッチ処理において、同日にリトライできるアプリケーションの提供を行う。 ※システムを長期間利用する中でデータ量が蓄積され、データ自体が肥大化した際にはデータ保存期間やスペックの見直しを協議する。

B.2.2.2	性能・拡張性	性能目標値	2	非N/A	仕様の対象としない	ベンダーによる提案事項	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					2	ガバメントクラウドに構築した標準準拠システムのバッチ処理において、同日にリトライできるアプリケーションの提供を行う。 ※システムを長期間ご利用する中でデータ量が蓄積され、データ自体が肥大化した際にはデータ保存期間やスペックの見直しを協議する。
C.1.1.1	運用・保守性	通常運用	1	定時内での利用（1日8時間程度利用）	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	繁忙期は定時外も頻繁に利用（1日12時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			2	ガバメントクラウドに構築した標準準拠システムは、自治体にヒアリングした上で、システム利用時間を設定するが、以下の時間内での利用となる。 7:00～20:00(最大22:00まで) ※22:00以降は、バックアップや連携処理の対応時間とする。
C.1.1.2	運用・保守性	通常運用	1	定時内での利用（1日8時間程度利用）	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用				2	ガバメントクラウドに構築した標準準拠システムは、自治体にヒアリングした上で、システム利用時間を設定するが、以下の時間内での利用となる。 7:00～20:00(最大22:00まで) ※22:00以降は、バックアップや連携処理の対応時間とする。
C.1.2.5	運用・保守性	通常運用	4	日次で取得	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、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		4	バックアップ頻度は、項番 A.1.3.1 RPO（目標復旧地点）で記載に準じて日次で取得とする。
C.4.3.1	運用・保守性	運用環境	2	情報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	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを利用する	情報システムの通常運用のマニュアルを提供ずる	情報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				2	ASPに必要な作業について、通常運用マニュアルおよび保守マニュアルを作成する。 また、当該作業のうち自治体にて作業が必要な場合には、自治体向けの操作マニュアルを提示する。
C.4.5.1	運用・保守性	運用環境	1	他システムと接続する	仕様の対象としない	ベンダーによる提案事項	他システムや外部システムと接続しない	他システムと接続する	外部システムと接続する					1	他システムとの連携が必要となるため、外部システムとの接続は発生する。
C.5.2.2	運用・保守性	サポート体制	2	アップデート	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート					2	ソフトウェアについては、弊社にてアップデートを実施する。 ※大規模な法改正対応については、保守作業内の対象外となる。
D.1.1.2	移行性	移行時期	4	利用の少ない時間帯（夜間など）	仕様の対象としない	ベンダーによる提案事項	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		4	土日夜間や停止可能な時間を予め協議した上で、システムを停止し移行を行う想定。
D.3.1.1	移行性	移行対象（機器）	3	移行対象設備・機器のシステム全部を入れ替える	仕様の対象としない	ベンダーによる提案事項	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			3	生活保護システムの動作に必要なシステム設定・ミドルウェアの設定を実施する。
D.4.1.1	移行性	移行対象（データ）	*	ベンダーによる提案事項	仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上				*	標準準拠システムへのデータ移行は、現行システムで保持するデータのみを対象とし、データ要件・連携要件標準仕様書の生活保護_基本データリスト【第2.1版】で定義された項目をデータ移行対象とする。現行システムで保持しないExcelデータ等は、原則としてデータ移行の対象外とする。 【移行対象】 ・生活保護システムデータ ・印影データ　※現在の印影を継続利用される場合 ・電子決裁・文書管理アップロードファイル ・タブレットアップロードファイル ※アクセスログなどの環境固有情報については移行対象外とする。
D.5.1.1	移行性	移行計画	1	ユーザとベンダーと共同で実施	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー					1	標準準拠システムへの移行作業は基本的にサービス提供側で実施する。移行テストの結果から、データクレンジングが必要なデータがある場合には、自治体側にてデータメンテナンスを実施する場合がある。また、システムで保有しているデータで、データ要件・連携要件標準仕様書の生活保護_基本データリスト【第2.1版】で定義されていないデータが存在する場合は、対象データをCSV形式で提供する。
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	1	制約有り（重要な制約のみ適用）	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）					1	以下のガイドライン等を順守して構築作業を実施する。 ・ISO/IEC 27001(ISMS) ・政府機関の情報セキュリティ対策のための統一基準 ・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省） ・プライバシーマーク
F.1.2.1	システム環境・エコロジー	システム制約/前提条件	1	制約有り（重要な制約のみ適用）	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）					1	以下のガイドライン等を順守して構築作業を実施する。 ・ISO/IEC 27001(ISMS) ・政府機関の情報セキュリティ対策のための統一基準 ・地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省） ・プライバシーマーク

■実現方法要求事項

項番	大項目	中項目	選択レベル		レベル								サービス提供選択レベル	共同利用方式の環境における選択レベル概要
					-	*	0	1	2	3	4	5		
A.3.1.1	可用性	災害対策	2	同一の構成で情報システムを再構築	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	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		2	機器を準備した環境にてシステムを構築するなど、自治体と協議の上、対応・調整とする。 AWS内（別アベイラビリティゾーンもしくは別リージョン）への構築を基本として対応する。
A.3.2.1	可用性	災害対策	2	1ヶ所（遠隔地）	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（近隣の別な建物と遠隔地）	2ヶ所（遠隔地）		2	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（東京リージョン）とは別のリージョン（大阪リージョン）へのバックアップを実施する。
A.3.2.2	可用性	災害対策	2	ネットワーク経由でストレージへのリモートバックアップを含む	仕様の対象としない	ベンダーによる提案事項	外部保管しない	媒体による外部保管のみ	ネットワーク経由でストレージへのリモートバックアップを含む				2	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（東京リージョン）とは別のリージョン（大阪リージョン）へのバックアップを実施する。
C.1.2.3	運用・保守性	通常運用	1	障害発生時のデータ損失防止	仕様の対象としない	ベンダーによる提案事項	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	職員の作業ミスなどによって発生したデータ損失防止				1	バックアップは日次で実施し、障害発生時には最新のバックアップデータから復旧する。
C.1.3.1	運用・保守性	通常運用	4	レベル3に加えてリソース監視を行う	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	レベル1に加えてエラー監視を行う	レベル2に加えてエラー監視（トレース情報を含む）を行う	レベル3に加えてリソース監視を行う	レベル4に加えてパフォーマンス監視を行う	4	生活保護システムの提供環境における障害検知を目的とした監視を実施する。 監視項目は、死活監視、エラー監視、リソース監視となる。 障害発生などにより定期的なパフォーマンスの確認が必要な場合は、パフォーマンス監視（モニタリング）を実施する。 サービス提供側の障害監視については、CSPのマネージドサービスを利用し監視を実施する。障害発生時にはCSPのマネージドサービスより適切な宛先に通知を行い、連絡・対応を実施する。
C.5.9.1	運用・保守性	サポート体制	3	四半期に1回	仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	3	標準準拠システムの運用保守状況について、サービス提供側から資料を送付し報告する。
C.5.9.2	運用・保守性	サポート体制	3	障害及び運用状況報告に加えて、改善提案を行う	仕様の対象としない	ベンダーによる提案事項	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	障害及び運用状況報告に加えて、改善提案を行う			3	標準準拠システムの運用保守状況について、サービス提供側から資料を送付し報告する。
C.6.2.1	運用・保守性	その他の運用管理方針	1	ベンダーの既設コールセンターを利用する	仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				1	サービス提供側のコールセンターを利用する。
C.6.3.1	運用・保守性	その他の運用管理方針	1	既存のインシデント管理のプロセスに従う	仕様の対象としない	ベンダーによる提案事項	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				1	既存のプロセスに従う。
C.6.4.1	運用・保守性	その他の運用管理方針	1	既存の問題管理のプロセスに従う	仕様の対象としない	ベンダーによる提案事項	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				1	既存のプロセスに従う。
C.6.5.1	運用・保守性	その他の運用管理方針	1	既存の構成管理のプロセスに従う	仕様の対象としない	ベンダーによる提案事項	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				1	既存のプロセスに従う。
C.6.6.1	運用・保守性	その他の運用管理方針	1	既存の変更管理のプロセスに従う	仕様の対象としない	ベンダーによる提案事項	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				1	既存のプロセスに従う。
C.6.7.1	運用・保守性	その他の運用管理方針	1	既存のリリース管理のプロセスに従う	仕様の対象としない	ベンダーによる提案事項	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				1	既存のプロセスに従う。
D.1.1.1	移行性	移行時期	4	2年未満	仕様の対象としない	ベンダーによる提案事項	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	4	移行期間は2年未満を前提に移行計画を策定する。
D.1.1.3	移行性	移行時期	1	有り	仕様の対象としない	ベンダーによる提案事項	無し	有り					0	移行時の職員様負担や作業の効率化を踏まえ、並行稼働は行わずに移行する。 並行は行わずに、運用テストフェーズに機能確認を実施する。
E.3.1.2	セキュリティ	セキュリティ診断	1	実施	仕様の対象としない	ベンダーによる提案事項	不要	実施					1	サービス提供側にてWeb診断を実施する。脆弱性が発見された場合、環境やシステムの修正を行い、対応する。 ・診断内容：Webアプリケーション診断 ・実施頻度：大幅な機能改修やミドルウェアやOSなどのバージョンアップ時に実施※予定