SLA 対策項目

１　全体

水道マッピングシステムをクラウド提供する範囲の保障事項を示す。

なお、水道マッピングシステムの利用のために活用する、既存の水道企業団の通信基盤及びセキュリティ等に関連するサービスは、本 SLA の対象外とする。

２　組織・運用編

(1) 情報セキュリティへの組織的取組の基本方針

ア　組織の基本的な方針を定めた文書

	対策項目
1	受注者の経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。 また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。
2	情報セキュリティに関する基本的な方針を定めた文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施すること。

(2) 情報セキュリティのための組織

ア　内部組織

	対策項目
1	経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。
2	従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。
3	情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

イ　外部組織（データセンタを含む）

	対策項目
1	外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施すること。
2	情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。

(3) 連携クラウド事業者に関する管理

ア　連携クラウド事業者から組み込むクラウドサービスの管理

	対策項目
1	連携クラウド事業者が提供するクラウドサービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携クラウド事業者によって確実に実施されることを担保すること。
2	連携クラウド事業者が提供するクラウドサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。

(4) 情報資産の管理

ア　情報資産に対する責任

	対策項目
1	取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。

イ　情報の分類

	対策項目
1	組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。

ウ　情報セキュリティポリシーの遵守、点検及び監査

	対策項目
1	各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。
2	クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。

(5) 従業員に係る情報セキュリティ

ア　雇用前

	対策項目
1	雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。

イ　雇用期間中

	対策項目
1	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。
2	従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続きを備えること。

ウ　雇用の終了又は変更

	対策項目
1	従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にすること。

(6) 情報セキュリティインシデントの管理

ア　情報セキュリティインシデント及びぜい弱性の報告

	対策項目
1	全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。

(7) コンプライアンス

ア　法令と規則の遵守

	対策項目
1	個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。
2	クラウドサービスの提供及び継続上重要な記録（データベース記録、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。
3	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。

(8) ユーザサポートの責任

ア　発注者への責任

	対策項目
1	クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者に起因するものであったとしても、発注者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施すること。

２　物理的・技術的対策編

(1) アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通する情報セキュリティ対策

ア　運用・管理に関する共通対策

	対策項目	評価項目	対策値
1	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。 稼働停止を検知した場合は、発注者に速報を通知すること。	死活監視インターバル（応答確認）	1 回以上/5 分
2	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。 障害を検知した場合は、発注者に速報を通知すること。	障害監視インターバル	1 回/10 分
3	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。 また、発注者との取決めに基づいて、監視結果を発注者に通知すること。	パフォーマンス監視インターバル	1 回/10 分
4	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。	–	–
5	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。	–	–
6	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	OS、その他ソフトウェア、ハードウェアに対するパッチ更新作業への対応	月例定例打合せにて協議
7	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して発注者等に報告すること。	定期報告の間隔	1 か月
8	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を発注者に対して行うこと。	第一報（速報）に続く追加報告のタイミング	翌営業日
9	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成すること。	–	–

(2) アプリケーション、プラットフォーム、サーバ・ストレージ

ア　アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理

	対策項目	評価項目	対策値
1	クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率を規定すること。 また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。	クラウドサービスの稼働率	99.5%以上
2	利用者の利用状況、例外処理の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。	利用者の利用状況の記録（ログ等）の保存期間	3 か月
		例外処理の記録（ログ等）の保存期間	5 年
		スタンバイ機による運転再開	可能 （ホットスタンバイ）
3	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。	ぜい弱性診断の実施間隔（アプリケーションのぜい弱性の詳細診断（外部委託、ドキュメントテストを含む）））	1 回/1 年

イ　アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策

	対策項目	評価項目	対策値
1	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。	更新間隔	1 回/月

ウ　サービスデータの保護

	対策項目	評価項目	対策値
1	利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。	バックアップ実施インターバル	1 回/1 日
		世代バックアップ	異なるサーバ／環境に合わせて 2 世代
2	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	バックアップ確認の実施インターバル （ディスクに戻してファイルサイズを確認する等）	1 回/年

(3) ネットワーク

ア　外部ネットワークからの不正アクセス防止

	対策項目	評価項目	対策値
1	ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。 また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。 また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。	–	–
2	発注者の情報システム管理者等の管理者権限の割当及び使用を制限すること。	–	–
3	利用者及び管理者（情報システム管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。	利用者のアクセス認証方法	記憶情報・所有情報・生体情報を組み合わせた多要素（二要素）認証
		情報システム管理者などのアクセス認証方法	記憶情報・所有情報・生体情報を組み合わせた多要素（二要素）認証
4	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。	–	–
5	不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS17/IPS18 の導入等）を講じること。	シグニチャ（パターンファイル）の更新間隔	1 回/1日

イ　外部ネットワークにおける情報セキュリティ対策

	対策項目	評価項目	対策値
1	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。	–	–
2	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	通信の暗号化	IP 暗号通信（VPN（Ipsec）等）又は HTTP 暗号通信（SSL（TLS）等）
3	第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。	–	–
4	外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。	通報時間	翌営業日

(4) ASP、クラウドサービス

ア　事業継続性

	対策項目
1	ASP、クラウドサービスで利用する、施設、システムは ISO22301(事業継続マネジメントシステム)の認証を得ていること。

イ　セキュリティ

	対策項目
1	ASP、クラウドサービスで利用する、施設、システムは ISO 27017（クラウドサービスのセキュリティ管理)の認証を得ていること。

ウ　個人情報保護

	対策項目
1	ASP、クラウドサービスで利用する、施設、システムは ISO 27018（クラウドにおける個人情報保護)の認証を得ていること。

(5) その他

ア　機密性・完全性を保持するための対策

	対策項目	評価項目	対策値
1	個人情報は関連する法令に基づいて適切に取り扱うこと。	-	-

イ　クラウド事業者の運用管理端末における情報セキュリティ対策

	対策項目	評価項目	対策値
1	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	パターンファイルの更新間隔	一週間以内
		OS、その他ソフトウェアに対するパッチ更新作業の着手までの時間	一週間以内

ウ　媒体の保管と廃棄

	対策項目	評価項目	対策値
1	紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	-	-
2	機器及び媒体を正式な手順に基づいて廃棄すること。	-	-