不法・危険盛土等衛星監視業務
仕様書（案）

令和７年３月

浜松市

目次

1. 本業務の背景と目的

1.1. 背景と目的

近年、不法・危険盛土等の崩落による被害が全国で報告されており、本市においても天竜区等で盛土の崩落による被害が発生する等、不法・危険盛土等への対応が喫緊の課題となっている。

令和 7 年度より、「宅地造成及び特定盛土等規制法」が全面施行され、市民の安心・安全を守るため、不法・危険盛土等に対して衛星画像を活用した盛土監視手法の整備を図るとともに、これら不法・危険盛土等を監視するため、ASP・SaaS を活用した盛土監視システムの調達を検討している。

2. 本業務の内容

2.1. 調達範囲

2.1.1. システム導入に係る調達範囲

本件における調達範囲を下記に示す。

図表－01 本業務における調達範囲

	区分	項目	特記事項
1	導入役務	✓ システム導入に係る役務	初期設定等
2	サービス提供	✓ サービスの提供	契約期間内

なお、以下の事項について留意すること。

- システム導入に係る調達範囲には、クラウドサービスの提供に加え、本市がサービスを利用するために必要となる作業（導入役務・運用保守）を含めるものとする。
- 調達するシステムのサービス提供期間は、導入後５年間を前提とすること。また、導入後５年間は提供見込みがあるサービスを提供すること。
- 過去３年以内に重大なセキュリティインシデント等が発生していないサービスを提供すること。

2.1.2. 盛土監視業務に係る調達範囲

本件における調達範囲を下記に示す。なお詳細については、「別紙 1_機能要件一覧」に基づく。

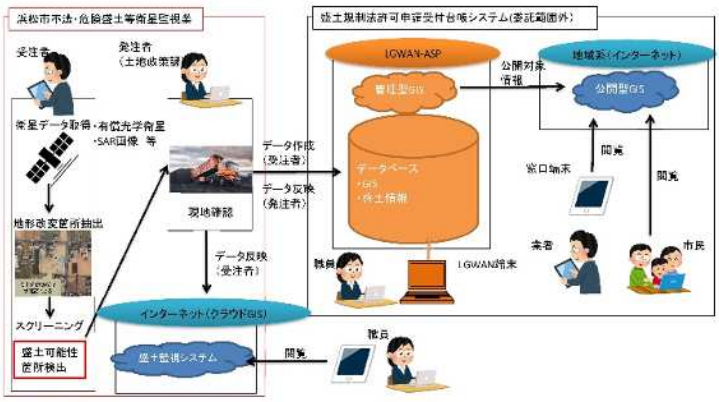
（１）業務項目

- 計画準備　　盛土抽出に向けた計画作成、衛星画像等の取得準備
- 改変箇所抽出　　二時期のデータ（衛星画像等）比較による地形改変箇所抽出
- システム設計　　盛土監視システム設計
- スクリーニング　地形改変箇所から、盛土の可能性がより高い箇所を抽出
- データ作成　　地形改変箇所、盛土可能性箇所の GIS データ作成
- 報告書作成　　作業内容について、報告書にとりまとめ
- 打合せ協議　　業務着手時 1 回、中間報告 2 回、成果品納入時 1 回

（２）成果品

- 業務完了報告書
- 報告書概要版データ
- 事業効果説明資料データ（パワーポイント 30 枚程度）
- 地形改変箇所、盛土可能性箇所の GIS データ

・図表－02　　システム構成図



2.2. 本市の想定する改善すべき問題点

本調達において新たな盛土監視システムの導入により、改善すべき問題点は以下のとおり。

- 市域が広く、市内全域の盛土を監視することが困難
- 職員によるパトロールと市民通報に頼る現状対応の限界
- 盛土発見の遅れによる対応の難航化

2.3. スケジュール

2.3.1. 履行期間

導入役務機関は契約締結日の翌日から、令和 8 年 3 月 31 日（火）までとする。なお、サービス提供期間は契約期間内とする。

・図表－03　　スケジュール案

令和 7 年度											
4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
公告		契約	初回画像取得				第２回画像取得				
											業務完了
		準備期間		システム構築					盛土抽出、スクリーニング		

3. 機能要件

3.1. 業務機能要件

3.1.1. 調達対象となる業務機能要件・帳票要件の一覧

本システムが備えるべき機能の要件は、「別紙 1_機能要件一覧」「別紙 2_帳票要件一覧」「別紙 3_連携要件一覧」にて提示する。

4.　非機能要件

4.1. 前提条件

本業務において導入するシステムは、クラウドサービス（ASP・SaaS）により提供されることを前提とする。

また、「浜松市 ASP・SaaS セキュリティチェックリスト」を満たすこと。なお、本システムは、LGWAN-ASP またはそれ以外のサービスいずれの提供形態でも許容する。

4.2. 利用環境

4.2.1.　システム利用時間

システム利用時間は以下のとおりである。

図表－04 システム利用時間

	分類	通常時利用時間帯
オンライン	平日	8:30～17:15
	土日祝祭日	-

4.2.2. システム利用者

システム利用者は本市職員（委託含む）である。

4.2.3. システム利用規模

システム利用者数、利用端末数、業務量は以下のとおりである。

図表－05 システム利用規模

項目	規模
システム利用者数	システム利用者：15 名程度 ・ 都市整備部盛土対策課 10 名 ・ 都市整備部北部都市整備事務所 5 名 システム管理者：3 名程度 ・ 都市整備部土地政策課 3 名 ※同時アクセス数は 2 程度を想定している。
利用端末数	・ 本庁：5 台 ・ 浜名区役所（外部拠点）：2 台

図表－06 事務処理件数（想定件数）

対象業務	対象作業	件数
盛土監視	盛土箇所閲覧	200 件
	盛土箇所印刷	50 件

4.3. システム利用環境

4.3.1. 端末

【現行の端末を利用する場合】

本システムが利用する端末は、現在本市にて使用している端末とすること。本市の端末の状況は、利用している OS が異なる等、複数の利用環境があることに注意すること。クライアント環境の一例を以下に示す。

図表－07 職員利用端末の仕様

区分	項目	仕様・導入ソフトウェア名等
ハードウェア	CPU	Intel Corei5 11 世代
	メモリ容量	8GB
	ディスク容量	6GB
	画面解像度	1366×768
ソフトウェア	OS	Windows 10 Pro
	ブラウザ	Microsoft Edge
	Office	Office 2016

なお、本システムは端末に搭載された Web ブラウザ（Edge（IE モード）、Google Chrome 等）から利用可能であり、かつシステムの利用にあたりアプリケーション等の追加インストール

を必要としないこと。
また、端末の OS や Web ブラウザの最新バージョンが公開された場合は、最新バージョンでも本システムが利用できるように、速やかにサポート対象とすること。

4.3.2. サービス提供環境

本業務で提供されるクラウドサービスは ISMAP（政府情報システムのためのセキュリティ評価制度）または ISMAP-LIU（ISMAP for Low-Impact Use）に登録されていることを原則とする。ISMAP または ISMAP-LIU に登録されていない場合は、クラウドサービスが構築されているデータセンターがデータセンターファシリティスタンダードのティア 3 以上に準拠しており、かつ、データセンターサービスを提供する事業者にて、情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づく ISMS 認証又はそれと同等の認証を取得していること。

なお、クラウドサービスが構築されているデータセンターは日本国内とする。

また、データセンター内にて、当該業務を行う場所及び情報を保管する施設その他情報を取り扱う場所において、入退室の規制及び防犯対策その他必要な情報セキュリティ対策を講じること。

4.3.3. ネットワーク

本システムは地域系ネットワークから利用できること。
また、「浜松市 ASP・SaaS セキュリティチェックリスト」を満たすこと。

4.4. 可用性要件

4.4.1. 継続性

システム構成の冗長化により、特定箇所に故障が発生した場合に業務への影響を局所化すること。

図表－08　継続性要件

対象	内容
RPO（目標復旧地点） （平常業務停止時）	業務停止を伴う障害が発生した際には、障害発生時点までのデータ復旧を目標とすること。
RTO（目標復旧時間） （平常業務停止時）	業務停止を伴う障害が発生した際には、6 時間以内でのシステム復旧を目標とすること。
RLO（目標復旧レベル） （平常業務停止時）	業務停止を伴う障害が発生した際には、全システム機能の復旧を実施すること。
システム再開目標 （大規模災害時）	情報システムに甚大な被害が生じた場合、情報システムは、1 カ月以内に再開することを目標とすること。
稼働率	年間のシステム稼働率は、99.9%を目標とすること。

4.4.2. 災害対策

地震、水害、テロ、火災などの大規模災害時や、ハードウェアの大規模障害の対策として、遠隔保管又は立地場所若しくは電源設備が異なるデータセンターでの冗長化を実施すること。

4.5. 性能・拡張性要件

性能・拡張性については、以下に示す「性能目標値」の内容を踏まえたシステムとすること。

図表－09　性能目標値

対象	内容
オンラインレスポンスタイム	オンラインレスポンスタイムは、ネットワークの遅延を除き、3 秒以内を目標とすること。

対象	内容
	なお、業務に支障のない状態を確保すること。
拡張性	「同時アクセス数」、「データ量」、「オンラインリクエスト件数」、「バッチ処理件数」については、1.2 倍程度となっても耐えうる拡張性を有すること。

4.6. システム監視要件

本市が求める監視要件は下記のとおり。なお、第三者が提供する IaaS／PaaS 環境等を用いて、サービスを構築している場合、当該第三者が下記に定める監視を実施していることをもって、本要件を満たしているとみなす。

図表－10　主な監視要件

対象	内容
各種ハードウェア（サーバ、ネットワーク、ストレージ）のハードウェア監視	SNMP Trap/Get 等
サーバの死活監視	ノード監視（Ping 監視等）、OS プロセス監視 等
サーバ上の OS レベルでのリソース監視	CPU 使用率、ストレージ空き容量 等
サーバ上のログ監視	OS のシステムログ 等

4.7. セキュリティ要件

以下に示す要件に留意し、セキュリティを担保すること。

図表－11　セキュリティ要件

要件	内容	
セキュリティ対策等	システムに保持する情報の機密性、可用性、完全性を維持するための最新の対策を十分に講じること。また、発注者がセキュリティ実施手順を策定もしくは改正する際はその作成を支援すること。 また、上記セキュリティ対策の遵守について、受託者の要員に対して、適切に教育・訓練等を行うこと。	
アクセス・利用制限	本システムは、利用者毎のアクセス管理が行われ、割り当てられた権限の範囲で操作可能な仕組みであること。	
データの秘匿	伝送データの暗号化の有無	伝送データについては、SSL／TLS 等の暗号化通信により第三者からの盗聴や改ざん等をされること無く安全に通信できること。
	蓄積データの暗号化の有無	蓄積データについては、認証情報を暗号化し管理すること。
ウイルス対策	本システムは、ウイルスやマルウェア等に対する対策を講じること。	
ログ対応	ログの取得	取得したログについて、漏洩、改ざん、消去等を防止できる機能を設けること。また、取得したログについて、本市の求めに応じて、提供できること。
	ログ取得の対象	セキュリティログ：アプリケーションログのうち、情報セキュリティに関連するログ（操作者、操作日時、操作内容 等）を想定している。システムへのログイン履歴及び成否等を記録した監査ログを含む記録。

要件	内容	
バックアップ・リストア	データ復旧の対応範囲	障害発生時のデータ損失防止策を講じること。 ※障害によりデータの損失が生じた場合、「RPO（目標復旧地点）」で定めた時点までデータを復旧すること。
	バックアップ自動化の範囲	バックアップの実施状況をシステム管理者が確認できること。バックアップが正常に終了しなかった場合、対応方針について本市と協議すること。
	バックアップ取得間隔	システム全体（OS、ミドルウェア、業務アプリケーション等）： 初期設定時、及びシステム更新時（改修、設定変更等実施時）に取得
個人情報保護	情報資産分類	機密レベルに応じた情報セキュリティポリシーが定められており、個人情報等は機密性の高い情報として、別途情報管理の仕組みが設けられていること。
	法令等遵守	個人情報保護法に従い、個人情報を管理すること。
	セキュリティ監査	定期的に本サービスに関するセキュリティ監査（内部監査または外部監査）を実施すること。
BCP 対策	大規模災害等の緊急時においても情報セキュリティ及び情報セキュリティマネジメントが適切に確保される仕組みを整備すること。	

5. 導入役務要件

5.1. プロジェクト管理要件

5.1.1. プロジェクト体制

業務実施にあたり受託者は本業務を確実に履行できる体制を設けること。

5.2. 研修要件

5.2.1. 研修の実施

システム管理者及びシステム利用者向けの操作マニュアルや説明動画等を用意すること。また、必要に応じて Q&A を提供すること。

5.3. 成果物

工程毎の成果物について、以下「図表－12　導入工程におけるドキュメント一覧」に示す。スケジュールは当該一覧の「納入時期」を目安とし、原則次工程着手前に現工程の成果物について作成を行い、承認を得るものとする。また、納入後１年間は、媒体破損、データ及びプログラム不良による納入物の再作成及び修正を保証できるように、受託者の責任において納入成果物の複製物を保管すること。

図表－12　導入工程におけるドキュメント一覧

工程	作成ドキュメント	内容	納入時期
導入準備	設定内容説明書	新システムを利用するにあたり、初期設定として登録する内容等をまとめたもの	初期設定前
研修	操作マニュアル	システム管理者及びシステム利用者向け操作マニュアル	本番稼動前
プロジェクト管理	議事録 連絡票	プロジェクトを運営するための各種書類	プロジェクト実施中

工程	作成ドキュメント	内容	納入時期
	その他発注者が指示する資料		随時

5.3.1. 納品形態及び部数

紙で2部（正本、副本）、電子で1部納入すること。

なお、電子データ提出時には、発注者が指定する納品書を合わせて提出するものとする。

また、成果品作成完了時点で最新のウイルスに対応したウイルス対策ソフトによりチェックを行い、使用したウイルス対策ソフト、チェックを実施した日付を明示した上で納品すること。

5.3.2. 納入場所

本市が指定する場所とする。

6. サービス提供要件

サービス提供業務について、以下に示す要件を実施すること。

6.1. サービス提供共通要件

6.1.1. サービス提供体制

後述する「対応時間」において、受託者は「図表－14 サービス提供業務一覧」に示す業務に対応可能な環境を準備すること。

6.1.2. 対応時間

以下のシステム利用時間帯での対応を基本とする。但し、翌日のオンライン運用に影響を与えると思われる場合は、本市と協議のうえ対応を決定する。

図表－13　システム利用時間

	分類	通常時利用時間帯
オンライン	平日	8:30～17:15
	土日祝祭日	－

6.1.3. サービス提供要件

サービス提供に係る業務について、以下に示す。

なお、本システムの構成要素として、他事業者のクラウドサービス（IaaS 等）・レンタルサーバ等が含まれている場合に、それらに起因して発生する各種運用保守業務も、受託者が窓口となり、受託者の責任において、全面的にユーザサポートすること。

図表－14　サービス提供業務一覧

業務	作業	内容
ヘルプデスク（問合せ対応）	受付	本市からの電話・メール等による問合せについて、受付・回答を行うこと。
	調査／回答	調査結果が既存事象であった場合には、速やかに回答すること。
セキュリティ管理	セキュリティ予防策の実施	セキュリティインシデントのリスクを低減させる予防策について、実施すること
	ウイルス・脆弱性対策管理	OS 等のセキュリティ脆弱性については、受託者にてセキュリティパッチファイルを提供・適用すること。

業務	作業	内容
障害時対応	障害調査	受託者は、障害発生内容の解析及び発生箇所を特定すること。
	暫定対応	受託者は、障害から復旧して業務を再開するために、暫定対応を行うこと。
	恒久対応	受託者は、障害の要因について対処し、同事象の発生を防止するために、恒久対応を行うこと。
	再発防止策／記録	受託者は、障害内容と対処内容を記録し、再発防止策を講ずること。
利用者管理	権限管理	アクセス制御等の権限管理は浜松市のシステム管理者にて実施するため、必要な助言を行うこと。

6.2. サービスレベル合意（SLA）

運用保守作業に関するサービスの内容と範囲、品質に関する要求水準と、それが達成できなかった場合のルールを含め、本市及び受託者間にて合意することとする。サービスレベル合意内容（SLA）は、「業務計画書」に明記するとともに、報告すること。なお、本調達により導入するクラウドサービスには、努力目標型の SLA を想定している。

SLA の要求水準が達成できなかった場合又は達成できない恐れがある場合は、原因を調査・分析し、できる限り改善すること。本市が想定する「サービスレベル項目（案）」を以下に示す。

図表-15　サービスレベル項目（案）

項目（案）	定義	目標値
オンライン稼働率	（「オンライン稼働時間」－「オンライン停止時間」）÷「オンライン稼働時間」×100　（%）	
	・24 時間 365 日	99.9%
稼働停止・障害検知時間	稼働停止、サービス障害を検知した場合は、本市担当職員に速報を通知するまでの時間	30 分以内
RTO（目標復旧時間）（業務停止時）	監視システムが故障を検知（ウイルス検知含む）した時間から回復するまでの時間	6 時間以内
問合せ回答率（即答件数／相談件数）又は問合せ回答待ち時間	本市職員から受託者の保守員に問合せを行う場合の回答指標	本市との SLA 締結時に協議
アプリケーション品質（変更作業等に伴う障害発生率（件数））	運用保守フェーズで実施した変更作業、軽微な改修案件数に対して、その案件を原因としたシステム障害の発生率（発生件数）	本市との SLA 締結時に協議
性能	通常時オンラインレスポンスタイム等において、著しい性能劣化と判定する場合の指標	本市との SLA 締結時に協議

7.　その他留意事項

7.1. 業務実施時における留意事項

・本市ネットワークの設定に変更が生じた場合には速やかに対応すること。

・本市及び第三者機関などによる監査・検査等が実施される場合は、本市の指示に従い資料作

成・実地調査・質疑応答など速やかに対応すること。
・すべての作業において、本市の業務、稼働中の業務システム等に影響を及ぼすおそれがある場合は、事前に明らかにし、本市の指示に従い作業を実施すること。
・本システムの運用管理要綱など、その他本システムの関連規程を遵守すること。
・受託者の都合により、本システムが提供するサービスの内容に変更が生じる場合は遅くとも1ヶ月以上前に、サービスが終了する場合は遅くとも6ヶ月以上前に、本市に対して告知を行うこと。
・受注者は、本契約に基づき発注者に本システムの利用を許諾するものとして、本システムの知的財産権その他の権利は受注者に留まることとする。

7.2. 関係法令等の遵守

受託者は、令和7年度不法・危険盛土等衛星監視業務に関係する法令等に基づいて適正に業務を遂行すること。

7.3. 法制度改正への対応

既存の法制度の改正について、基本的にソフトウェアのバージョンアップや機能追加等により対処し、サービス提供業務の標準対応の範囲に含まれるものとする。

7.4. 支払い方法

受注者は業務の履行が完了した場合において、発注者あてに支払請求書（当該年度分）を送付することとし、発注者は契約書に定める当該期に係る契約金額を支払うこととする。

7.5. 業務の契約終了・引き継ぎに関する事項

本業務の契約履行期間の満了、全部もしくは一部の解除、またはその他契約の終了事由の如何を問わず、本業務が終了となる場合には、受託者は本市の指示のもと、本業務終了日までに本市が継続して本業務を遂行できるよう必要な措置を講じるため、業務引き継ぎに伴うシステム移行等に必要となる構成要素を円滑に提供できるようにすること。なお、移行用のコンテンツ等の提供に係る費用は本契約に含まれるものとし、新たな費用は発生しないものとして取り扱うこと。移行用のコンテンツ等は二次利用できるように、汎用的なデータ形式で出力して、本市に提供すること。

また、契約終了から一定の期間内において、本システム内の本市作成データを消去すること。

以上

別紙1　機能要件一覧　　（様式6　システム機能要件チェックリスト）

機能名称			機能の定義	重要性	チェック	実現方法	配点
1. 盛土抽出							
1.1.抽出条件							
	1.1.1.	抽出面積	面積500m2以上の地形改変箇所が抽出可能である。	A			4
	1.1.2.	期間	二時期のデータ（衛星画像等）比較により、期間内の新たな地形改変箇所の抽出が可能である。	A			4
	1.1.3.	画像取得（１回目）	撮影日が、令和7年5月26日から3か月以内の画像取得が可能である。	A			4
	1.1.4.	画像取得（２回目）	撮影日が、1回目画像の撮影日から4か月以降の画像取得が可能である。	A			4
	1.1.5.	画像取得範囲	市内全域の画像を取得し、抽出作業を行うこと。撮像範囲のうち、視認できない範囲は、市域の10%未満とすること。	A			4
1.2. 地形改変箇所情報の提供							
	1.2.1.	面積	地形改変箇所の面積を計測可能である。（100m2単位）	A			4
	1.2.2.	位置情報	地形改変箇所の位置情報について、位置図を用いて、地番及び緯度経度の提供ができる。	A			4
	1.2.3.	関連情報	地形改変箇所に関する情報として、関係法令（宅地造成及び特定盛土等規制法、都市計画法、森林法、砂防三法等を想定）の規制区域であるか、既存盛土及び大規模盛土造成地等の既知の盛土箇所であるかどうか、判断ができる。	B			2
	1.2.4.	GISデータ化	他システム等での利用が可能なよう、地形改変箇所毎の概形、面積、地番及び抽出理由をシェイプファイル形式で提供すること。	A			4
	1.2.5.	盛土情報の提供	発注者に対して、上に記載の地形改変箇所情報と抽出理由を箇所毎にとりまとめ、報告書に記載すること。	A			4
1.3. スクリーニング							
	1.3.1.	許可情報による精査	地形改変箇所について、既存の法令許可情報により、盛土であるかの精査ができる。	A			4
	1.3.2.	地形情報による精査	地形改変箇所について、地形図の確認により、盛土であるかの精査ができる。	A			4
	1.3.3.	航空写真による精査	地形改変箇所について、航空写真の確認により、盛土であるかの精査ができる。	A			4
1.4.業務引継ぎ							
	1.3.1.	次年度業務への引継ぎ	盛土監視業務が次年度以降も実施されることを考慮し、盛土可能性箇所データ等をとりまとめ、次年度業務への円滑な引継ぎが可能である。	A			4
	1.3.2.	画像情報	盛土監視業務が次年度以降も実施されることを考慮し、取得した衛星画像の確認及び提供が可能である。	A			4
2.閲覧システム							
2.1. 共通							
	2.1.1.	ログイン	ユーザーID及びパスワードにより認証を行う	A			4
	2.1.2.	ログアウト	アプリケーションを終了させると同時にログアウトされる（自動ログアウト）	B			2
2.2. 閲覧							
	2.2.1.	移動	全方向へのスクロールができる。	B			2
	2.2.2.	拡大縮小	マウスやボタン等で拡大縮小ができる。	B			2
	2.2.3.	計測	指定箇所の座標、延長、面積の計測が可能である。	B			2
	2.2.3.	画面表示	画面上で地形改変箇所を確認できる。	A			4
	2.2.4.	情報表示	地形改変箇所情報の表示ができる。	A			4
	2.2.５.	表示画像	光学衛星画像、地形図、地番図の画像を確認できる。	B			2
2.3. 検索							
	2.3.1.	盛土番号	任意の盛土番号により、地形改変箇所の検索ができる。	A			4
	2.3.2.	場所	地番又は住所から、地形改変箇所の検索ができる。	B			2
	2.3.3.	時期	盛土時期から、地形改変箇所の検索ができる。	B			2
2.4. 印刷							
	1.3.1.	画面印刷	表示画面の印刷ができる。	A			4
	1.3.2.	日付入力	印刷した際に、印刷時点の日付が入力される。	B			2
2.5.登録							
	2.3.1.	新規登録	地形改変箇所情報について、新規登録が可能であること。	B			2
	2.3.2.	修正	地形改変箇所情報について、修正が可能であること。	B			2
	2.3.3.	削除	地形改変箇所情報について、削除が可能であること。	B			2

凡例

A 必須要件　実現が必須である。

B 任意要件　実現必須ではないが、実現できることが望ましい。

		得点掛率
○	システム標準機能で実現	×１
△	代替機能又は、類似機能にて実現	×1/2
×	実現不可	×０

別紙2 帳票要件一覧

No	帳票名称	帳票概要	機能一覧との対応	実現方法	媒体	出力形態	出力頻度	出力頻度毎出力枚数	印刷場所	様式	電子公印使用有無	用紙種別	用紙サイズ	サンプル有無	重要性	留意事項
1	盛土箇所図	閲覧システム上から、システム画面を印刷したもの。		4：非定型（汎用ﾌｧｲﾙ出力（EUC機能）等の出力で可）	紙・電子	個別	随時	1	職場内	指定なし	なし（-）	汎用紙	A4	なし（-）	A	印刷日時が印字されること。
2																
3																
4																
5																
6																
7																
8																
9																
10																
11																
12																
13																
14																
15																
16																
17																

別紙3　連携要件一覧

No	システム名	方向	連携先システム名	連携媒体	連携方式	連携方式（その他）	連携頻度	連携情報名・内容	備考
記入形式	自由記述	択一	自由記述	択一	択一	自由記述	択一	自由記述	自由記述
1	不法危険盛土等衛星監視業務	→	盛土規制法許可申請受付台帳システム	システム	ファイル連携	シェイプファイル	随時	盛土区域、箇所、情報	
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									

別紙4　浜松市ASP・SaaSセキュリティチェックリスト

各チェック項目の充足有無を"回答"欄にご回答ください。また、そのように考える根拠を"回答根拠"欄にご回答ください。

【回答凡例】○：チェック項目を満たす　×：チェック項目を満たさない　△：本市と相談が必要(例：チェック項目は満たさないが、代替策により同水準のセキュリティレベルの確保が必要な場合 等)

事業者名：

システム名：令和7年度不法危険盛土等衛星監視業務　閲覧システム

チェックリスト				事業者回答	
No	分類	チェック項目		回答	回答根拠(対応状況、実現方法 等)
例	○○	○○の対策が実施されていること。		○	当社サービスでは○○の機能を有しており、本機能で○○できることから、本チェック項目を満たすと考える。
（1）セキュリティに関するチェックリスト					
1	人的対策	組織として情報セキュリティポリシーが定められており、全ての従業員等に対して、適切な教育・訓練等を実施することにより、ポリシーの遵守が徹底されていること。			
2	ファシリティ	本サービスで扱うデータは、日本国内のデータセンタでのみ保管されること。			
3	アクセス制御	正当な権限を有する利用者のみがサービスや機能を利用できるように、アクセス制御ができること。			
4	保管データの暗号化	本サービスで扱うデータを保護するために、保管データの暗号化による対策が実施されること。			
5	通信の暗号化	本サービスで扱うデータの通信において、データの盗聴、改ざん等から保護するために、通信の暗号化による対策が実施されること。			
6	証跡管理	情報セキュリティインシデント等発生時にその原因分析等ができるよう、利用者の活動等に係るログが管理されること。			
7	マルウェア対策	マルウェアから保護するために、マルウェアの検出、予防、回復のための対策が実施されること。			
8	脆弱性対策	本サービスに関係する技術的脆弱性に関する情報を速やかに入手するとともに、当該脆弱性に対する対応策が検討・実施されること。			
9	BCP	大規模災害等の緊急時においても情報セキュリティ及び情報セキュリティマネジメント継続のためのルールが組織的に策定されていること。			
10	サービス終了時のデータ消去	本サービスの利用終了から一定期間以内に本市データが完全に消去されること。			
※No11～16は本サービスで個人情報を扱う場合のみご回答ください。					
11	情報資産分類	機密レベルに応じた情報セキュリティポリシーが定められており、個人情報等は機密性の高い情報として、別途情報管理の仕組みが設けられていること。			
12	個人情報保護法等遵守	個人情報保護法及び関連するガイドラインの要求事項に従った個人情報保護管理が実施されること。			
13	重大インシデント	過去3年以内に、個人情報に関する重大なインシデントが発生していないこと。			
14	IPアドレス認証等	ID/パスワードに加え、IPアドレス等他要素によるアクセス制御ができること。			
15	個人情報に関するロ	個人情報の入力・出力に係るシステムログ(操作者、操作日時、操作内容)が管理されること。			
16	セキュリティ監査	定期的に本サービスに関するセキュリティ監査(内部または外部)が実施されている			
※No17は本サービスのシステム構成要素として、他事業者のサービスを含む場合のみご回答ください。					
17	サプライチェーン	本サービスのシステム構成要素として、他事業者のクラウドサービス・レンタルサーバ等が含まれている場合も、本サービスのセキュリティインシデント等の発生においては、全面的に貴社にてユーザサポートが実施されること。			
（2）その他要件に関するチェックリスト					
18	データの所有権	本市が本サービスで扱うデータの所有権は本市に帰属すること。			
19	バックアップ	障害が発生した際に、適切にデータ復旧ができるように、本サービスの中で、バックアップができること。			
20	動作環境	本サービス利用に際して、クライアント端末側では標準ブラウザを除くソフトウェアやプライグインのインストール、OSやブラウザ等の設定変更が必要ないこと。			
21	最新OS等への対応	最新バージョンのクライアント端末側OSやブラウザを速やかにサポート対象とするこ			
22	法制度改正対応	既存の法制度の改正対応は、サービスのバージョンアップ等により本サービス提供の範囲内で実施されること。			
23	サービス変更通告	サービス提供者の都合により、サービスの内容を変更する場合は、本市に対して、遅くとも1ヶ月以上前に、その旨と通知すること。			
24	サービス終了通告	サービス提供者の都合により、サービスを終了する場合は、本市に対して、サービス終了の遅くとも6ヶ月以上前に、その旨を通知すること。			
25	サービス終了時のデータ移行	本サービスの利用終了に際して、サービスで保管されているデータを二次利用できるように、汎用的なデータ形式で出力して、本市に引き渡せること。			
（3）【参考】認証取得状況 ※あくまで参考に回答を求めるものであり、下記の認証取得を必須とするものではありません。					
26	認証取得	右記の認証取得状況を回答してください。	ISMAP		
			Pマーク(プライバシーマーク)		
			ISO27001		
			ISO27017		
			ISO27018		

個人情報の取扱いに係る特記事項

受託者は、個人情報の保護に関する法律（平成１５年法律第５７号）に基づき、個人情報を取り扱う際には、以下の事項を遵守しなければならない。

１　受託者は、この契約の履行に関して知り得た秘密を漏らしてはならない。この契約が終了した後も同様とする。

２　受託者は契約の履行に関して知り得た個人情報について、委託者が指定した目的の範囲内でしか利用してはならない。

３　業務完了後、委託者の指示により保管を要するものとされた個人情報は、委託者が指定した目的の範囲内で使用することができる。ただし、委託者がその利用を停止するように求めたときは、受託者は直ちに利用を停止しなければならない。

４　受託者は業務上の目的で個人情報を取り扱う場合であっても、次の各号に掲げる行為を行う場合については、当該行為を行うことができる場合を必要最小限に限定しなければならない。

(1) 個人情報を複製する場合

(2) 個人情報を送信する場合

(3) 個人情報が記録されている媒体の外部への送付又は持ち出し

(4) その他個人情報の適切な管理に支障を及ぼすおそれのある行為

５　受託者は組織的安全管理措置として次の各号に掲げる措置をとらなければならない。

(1) 組織体制の整備

(2) 個人情報の取扱いに係る規律に従った運用

(3) 個人情報の取扱状況を確認する手段の整備

(4) 漏えい等の事案に対応する体制の整備

(5) 個人情報の取扱状況の把握及び安全管理措置の見直し

６　受託者は人的安全管理措置として、従事者に必要な教育をしなければならない。

７　受託者は物理的安全措置として、次の各号に掲げる措置をとらなければならない。

(1) 個人情報を取り扱う区域を限定しなければならない。

(2) 個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行わなければならない。

(3) 個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、委託者の許可を得るとともに、パスワード等を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置をとる。

８　受託者は技術的安全管理措置として次の各号に掲げる措置をとらなければならない。

(1) 当該個人情報にアクセスする権限を有する者の範囲と権限の内容を、業務を行う上で必要最小限の範囲に限定しなければならない。

(2) アクセス権限を有しない者は、個人情報にアクセスしてはならない。

(3) アクセス権限を有する場合であっても、業務上の目的以外の目的で個人情報にアクセスしてはならず、アクセスは必要最小限としなければならない。

(4) アクセス状況を記録し、その記録を一定期間保存し、及びアクセス記録を定期的に分析しなければならない。また、アクセス記録が改ざんされないように必要な措置をとらなければならない。

(5) 外部からの不正アクセスを防止するため、必要な措置をとらなければならない。

(6) 個人情報を含む電磁的記録又は媒体の誤送信・誤送付、又はウェブサイト等への誤掲載を防止するため、個別の事務・作業において取り扱う個人情報の秘匿性等その内容に応じ、複数の従業員による確認やチェックリストの活用等の必要な措置をとる。

9　受託者は、個人情報の漏えい等の事案が発生した場合は、直ちに委託者に通報するとともに、その詳細について書面をもって報告しなければならない。あわせて、漏えいした個人情報の拡散を防止する等の必要な措置をとらなければならない。

10　受託者は、個人情報又は個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、業務責任者の指示に従い、一切の個人情報を溶解、焼却、切断等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。その際に委託者が立ち会いを求めた時は、業務に特別な支障を生じることがない限り拒むことはできない。

11　前項の規定により、廃棄を実施した場合は、その処分内容を書面により委託者に報告しなければならない。また、保有した個人情報をそのまま返却する場合においても同様に報告しなければならない。

12　受託者は、委託者の求めに応じ、個人情報の管理体制及び実施体制や個人情報の管理の状況について、報告しなければならない。また、業務に特別の支障を生じる場合を除いて、委託者が実地検査を求めたときはこれに応じなければならない。

13　受託者は、業務の一部を再委託（再委託先が委託先の子会社である場合も含む。）する場合には、個人情報の取扱いについて第1項から第10項までの措置をとるように委託先を監督しなければならない。