仕　様　書

１　件名　草加市道路維持管理システム導入

２　目的

草加市道路維持管理システムの導入により、道路パトロール業務の効率化及び要望受付機能の一元管理をすることを目的とする。

３　実施期間

契約締結日から令和８年（２０２６年）３月３１日まで

４　支払方法

業務完了払

５　道路持管理システムについて

草加市内における道路維持管理業務の効率化と高度化を図るため、スマートフォンとクラウドを活用した道路維持管理システムを構築するものとする。

期限については、令和７年１１月３０日までに構築するものとし、その後試行期間としてシステムを運用するものとする。

６　基本事項

⑴　システム形式

システム形式は、インターネット経由でクラウドサービス事業者が提供するサーバやソフトウェアを利用する「クラウド型」とする。

⑵　システムサービス実施の前提条件

①　サービス利用環境

以下の機器及びネットワークサービス（以下「発注者環境」という。）において、本システムを利用するものとする。

ア 草加市役所建設部維持補修課（以下「発注者」という。）から接続可能なインターネット環境（埼玉県自治体情報セキュリティクラウド）

イ 発注者のパソコン及びプリンター

ウ 発注者のパソコンで利用するWebブラウザはMicrosoft Edge、Google Chromeとする。

⑶　セキュリティ対策の実施

受注者は本システムへの不正アクセスやデータ改ざん、情報漏洩などのセキュリティ事故の防止に努め、別記「外部委託における情報セキュリティ遵守事項」の内容を実施するものとする。また、本サービスにおけるセキュリティ事故の発生を確認した場合は、発注者に報告するとともに、必要な対処を行うものとする。

⑷　システムサービスの中断及び停止

試行期間内においてシステムのメンテナンスや緊急時などやむを得ない事情により本サービスの提供を中断または停止した場合は、その後の対処について両者協議の上決定するものとする。

⑸　システムサービス終了時のデータの取り扱い

本サービスの終了時において、受注者は速やかに本サービスに登録（入力）したデータを発注者に返却し、発注者の指示により消去専用ソフトにて消去をし、消去完了を証明する証明書を提出すること。なお、返却方法及び返却期日については両者協議の上決定するものとする。

⑹　そのほかのデータの取り扱い

発注者が本システムサービスで入力したデータ（コンテンツ）について、受注者は発注者への確認及び許可なく改変しないものとする。

⑺　知的財産権の帰属

本サービス及び本サービスに関連するソフトウェア等の著作権は受注者に帰属するものとする。ただし発注者は本サービスを利用するために必要な範囲で、それらのソフトウェア等（受注者が秘密である旨表示したものを除く）の全部または一部を複製することができるものとする。

⑻　システムサービスの基本内容

①　初期設定等のサービス

本システムを使用するためのユーザーIDとパスワード（以下「ユーザーID」という。）の発行通知及びクラウドシステム環境等の環境構築を行うものとする。

②　ログイン機能

以下の機能が利用できるものとする。

ア ログイン機能

(ｱ) 本システムの利用者はログイン ID・パスワードによって管理され、ログイン画面でIDとパスワードを要求・認証すること。

(ｲ) ログイン認証後、認証トークンを発行し、ログイン以降のアクセスについて認証トークンが保持されているアクセスであることを確認する機能を有すること。

イ メニュー画面

(ｱ) 利用者毎に機能メニューへのアクセス制御が行われ、利用者毎に利用可能なメニュー表示を行う制御機能を有すること。

③　借上機器の扱い

発注者は、受注者から基本サービスの利用に必要なスマートフォンを借上げ、それらの機器を通じてインターネット通信サービスの提供を受けるものとする。(機器の仕様と通信の仕様は「７．道路維持管理支援システム要件　３ システム利用要件を参照」)

ア 機器の借上期間

貸与期間は令和７年１２月１日から令和８年３月３１日

イ 借上機器の引き渡し

サービス開始時のこれらの借上機器の引き渡し方法は、両者協議の上決定するものとする。

ウ 使用保管管理

発注者は、これらの借上機器を、善良な管理者の注意をもって管理するものとする。

エ 保証

(ｱ) 保証期間等

保証期間は、上記アの借上期間とする。詳細については、両者協議の上、決定するものとする。

⑼ システム想定利用者数等

本システムについては、拠点箇所を草加市役所維持補修課内とし、1日あたりの職員の想定利用者数等について、以下のとおりとする。

項目	想定数	備考
利用者数（職員）	22人	
スマートフォン(職員用)	3台	補修係2台　占用係1台
スマートフォン (パトロール車等)	5台	パトロール車及び作業車1台あたり1台

⑽ 初期導入

①本システムは、令和７年１１月３０日までにシステム構築が完了し、道路パトロール日誌作成の運用が可能になるように携帯端末の配布を行う。

②受注者は道路パトロールの運用者を対象に、運用開始前に操作説明会を開催する。

7　道路維持管理支援システム要件

⑴　システム基本方針

①　要望受付管理機能

・Web 上で住民自らが入力した要望内容を元に自動で受付登録
・その他、電話やメール等で受けた要望内容の受付登録
・受付票に写真や地図の添付が可能
・登録された受付内容はリアルタイムで事務所内職員とパトロール班に情報共有が可能

②　道路パトロール日誌作成機能

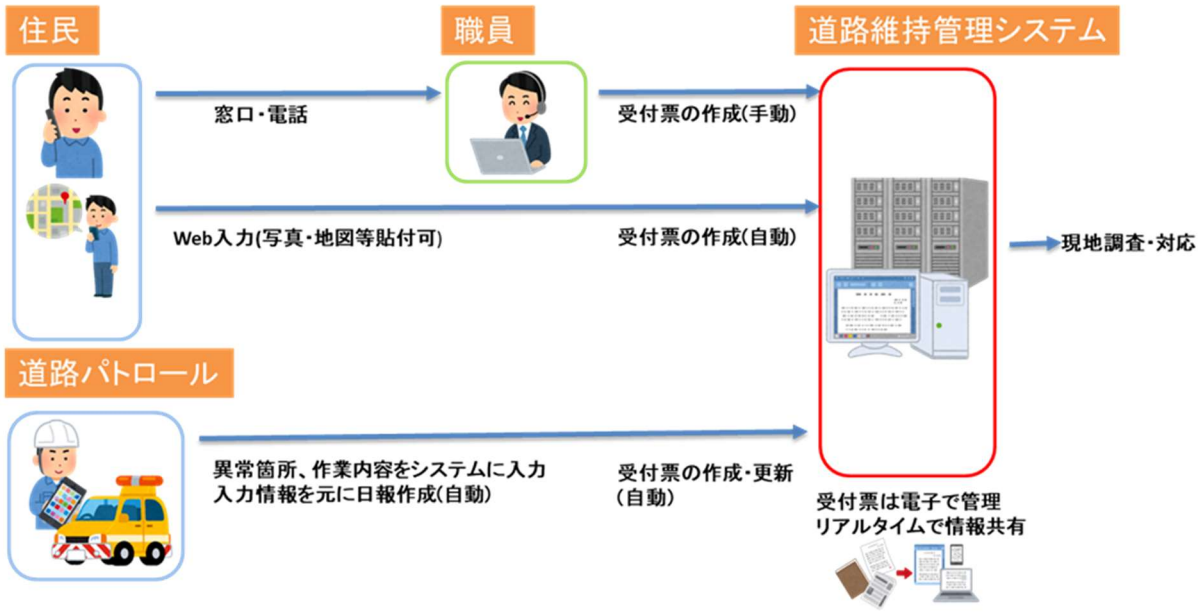
・パトロール中に写真撮影など現地確認した結果をシステム内に記録
・パトロール記録はリアルタイムで事務所内職員との情報共有が可能
・パトロール情報を元にパトロール日誌の帳票を自動作成し、システム内で供覧可能。

③　データ管理機能

・登録されたパトロール情報及び要望受付内容を地図画面上に表示
・表示される受付内容は項目ごとにレイヤー管理・色分けしたマーカーで表現することで、緊急対応案件等が一目で確認でき、迅速な情報共有が可能

⑵　システム概要

①　道路維持管理システム概要を下記に示す。



② システム機能の概要を下記に示す。

(表1) 機能概要一覧

No	機能		概要
1-1	要望受付	要望受付記録	・要望内容を記録する入力フォーム ZENRIN住宅地図を背景とした位置図登録機能付き ・ Web上で住民自らが入力した要望 内容を元に自動で受付登録 ・その他、電話やメール等で受けた要望内容の 受付登録 ・受付票に写真や地図の添付が可能
1-2		受付票作成	・要望受付記録に基づき受付票を自動作成 行政報告等の集計が簡単に出力可能
1-3		情報連携	・パトロール記録用のスマートフォンアプリ上に 要望受付地点を異状箇所として取り込み可能
2-1	パトロール	パトロール記録	・パトロール記録用のスマートフォンアプリケーション 要望や事故受付地点へのナビゲート支援機能付き スマートフォンアプリの背景に ZENRIN住宅地図を表示
2-2		報告書自動作成	・パトロール記録に基づき、パトロール日誌を自動作成 時系列明細（確認場所、異状内容、対応内容等出力） 走行経路図（GPSに基づいた走行経路を地図上に出力） 異状位置図（ZENRIN住宅地図を背景に、異状箇所出力） 写真台帳（異状箇所の処置前後の写真出力）
3-1	事故受付	事故受付記録	・事故受付内容を記録する入力フォーム ZENRIN住宅地図を背景とした位置図登録機能付き
3-2		受付カード作成	・事故受付記録に基づき受付カードを自動作成 項目ごとの集計が簡単に出力可能
3-3		情報連携	・パトロール機能に事故受付場所・内容を取り込み可能
4-1	データ管理	情報照会・検索	・異状記録や苦情内容などの蓄積データを条件検索・照会 検索結果のCSV出力機能付き
4-2		地図表示・分析	・ZENRIN住宅地図など地図レイヤー表示 ・道路網、異状箇所などを地図上に表示 対応状況など を地図上でフィルタリング、集計可能
4-3		データ集計	蓄積データに基づく実績報告や月報集計など自動集計
4-4		写真・ファイル管理	パトロール日誌などに関連する画像ファイル等を保存・管理

⑶　システム利用要件

①　スマートフォンのスペック

パトロール記録に利用するスマートフォンのスペックを表２に示す。

(表2) スマートフォンのスペック

サイズ（幅×高さ×厚さ）	71㎜×　153㎜×8.4㎜ 程度
ディスプレイ	6.1インチ程度
内蔵メモリ（ROM／RAM）	ROM 128GB UFS 2.2／RAM 6GB LPDDR4X
データ通信量	一般に提供する通常速度において使用できるデータ通信量が１台・１月あたり３ＧＢ以下
機能等	・生活防水以上の防水・防塵性能を備えること ・Android OS を搭載した携帯端末であること ・データ通信機能を備えること ・カメラ機能を備えること ・道路維持管理システムが利用可能であること ・GPS 機能を備えること ・紛失や盗難時に遠隔操作によるロック、データ消去等ができる機能を備えること
その他	・付属品　AC アダプター、USB コード ・費用は通信費と端末及び付属品代金等をまとめて月額定額の形とする ・契約事務手数料等は上記月額定額料金に含む ・端末および付属品の破損や不具合時、紛失の補償を含む、ただし故意の破損や明らかな管理不備などの場合は補償の対象外とする

⑷　性能・信頼性要件

性能・信頼性要件について、受注者と SLA（Service Level Agreement、サービスレベル合意）で保証するサービスレベルを定義する。SLA の案を表３に記載する。

（表３）信頼性に関する SLA（案）

項番	大分類	中分類	小分類	サービス内容	品質目標値(想定)
1-1	可用性	サービス提供管理	サービスの提供	サービス提供時間帯は24時間365日 （ただし、サービス環境のメンテナンス等の都合による一時的停止は除く）	稼働率99%以上
1-2			計画停止予定通知	具体的な停止日時、時間については、 システム画面上で事前通知	1ヶ月以上前までに通知 （緊急性を要するメンテナンス時や事前に承認を得た計画停止は除く）
2-1	信頼性	障害対応	障害通知	提供サービスに何らかの障害発生した時の通知を行う	障害検出から通知までの時間 サポートサービス時間帯：検出後60分以内 サポートサービス時間外：翌サポートサービス時間開始後60分以内
2-2			復旧対応	障害復旧作業を行う	障害復旧作業時間 サポートサービス時間帯：8時間以内 サポートサービス時間外：翌サポートサービス時間開始後8時間以内 但し、8時間以内の復旧の目途が立たない場合は、別途対応日程と対策を協議し復旧方法と目途を決定する
2-3			障害報告	障害発見から障害復旧、再発防止計画まで情報を報告書にまとめ提出する	障害復旧後5営業日以内に報告書提出
2-4		バックアップ管理	バックアップ作業	システム全体のバックアップを行う	システムイメージバックアップ1日1回（自動）、7世代管理 （バックアップ異常発生時　翌サポートサービス時間開始後すみやかに実施）
2-5				データのバックアップを行う	データバックアップ　1回/日（自動）、7世代管理 （バックアップ異常発生時　翌サポートサービス時間開始後すみやかに実施）
2-6		HDD容量	HDD標準使用上限	データ保管期間を5年分のHDDを用意する。	300GB以上
2-7		時刻同期	時刻同期	データセンター内のサーバ間の時刻同期を行い、定期的に確認を行う	1回／日
2-8		サーバネットワーク監視	サーバ・ネットワーク監視	定期的にデータセンター内の提供サービスを構成する各機器の稼動状況の監視を行う 運用監視ツールを利用し、コマンドにより応答確認を行い、稼動状況の監視を行う	1回／15分
2-9			DB環境監視	提供サービスに必要となるデータベース環境について、障害予防の観点から定期的に動作環境の確認を行う	1回／週
2-10		ウィルス対策管理	パターンファイルの更新	最新の検索エンジンやパターンファイルを入手し、提供サービスを構成するサーバ機器へ配信・適用する仕組みを搭載しているウィルス対策ソフトを利用する。	1回/日
2-11			通知体制	ウィルス対策ソフトによるウィルスチェックの結果、ウィルス発見時にシステム管理者に対する通知を行う	ウィルス発見時には30分以内にシステム管理者に対してメールにて通知を行う
2-12			駆除体制	ウィルス対策ソフトによるウィルスチェックの結果、ウィルス発見時には対策を開始し、最終完了報告を行う（サーバのみクライアントは除く）	対策開始までの時間 サポートサービス時間帯：発見後30分以内 サポートサービス時間外：翌サポートサービス時間開始後30分以内 上記対策完了後、最終完了報告を行う。
2-13		セキュリティホール	セキュリティホール対策	ベンダーより通知のあったセキュリティホール情報に基づき対応方針を協議し対策を行う 対策適用結果について定期的な報告を行う	報告は必要と判断した場合、5営業日以内に対応方針の報告 セキュティパッチ適用要否を判断し、必要な場合、ベンダリリースから1ヶ月以内に実施
3-1	サービスサポート	問合せ	問合わせ対応 ヘルプデスク	サポート窓口の設置	電話受付：平日9時～17時（土・日・祝日及び別に定める休日を除く） メール受付：24時間
3-2		運用計画	運用計画策定	提供サービスの業務利用にあたり運用計画表の作成を行う	サービス開始（更新）前月末までに年間スケジュールを提示
3-3		定例会議	状況報告	四半期の運用状況を報告し、次の四半期の運用スケジュール確認を行う	定例会議 4半期に1回。参加者・報告形式は別途協議
4-1	保守	機能改善	レベルアップ回数	機能修正、改善等レベルアップ 但し、仕様変更や個別カスタマイズは除く	1回/年以上
5-1	処理性能	画面表示	通常画面表示速度	端末での各種業務処理画面の表示に要する時間（メニュー、検索条件指定画面、地図表示画面など）	3秒以内 但し、通信環境の問題による遅れ、帳票作成時の画像や地図データを扱う処理等は除く
5-2		更新処理	データ更新処理速度	端末でのデータ1件の更新・追加・削除に要する時間	6秒以内 但し、通信環境の問題による遅れ、帳票作成時の画像や地図データを扱う処理等は除く
5-3		照会処理	データ照会処理速度	端末でのデータ1件の照会に要する時間	
5-4		検索処理	コード検索処理速度	端末でのコード検索・表示に要する時間	

上表に加え、関連事項として下記も要件とする。

①　ログの取得

本サービスへの不正アクセスや故障の原因調査のために、サービスのアクセスログ、システムログを取得し、1 年間保管するものとする。

② トラブル発生時の措置

本サービスが正常に提供されない等のトラブルを検知したときは、次の事項を実施するものとし、必要な対処を行うに際して、相互に可能な協力を誠実に行うものとする。

発注者からのトラブルの連絡を受けたときには、当該トラブルの原因所在の調査を行うものとする。その結果、本サービスに原因がある場合、受注者は必要な対処をとるものとする。

発注者は、発注者の接続回線環境、発注者環境に原因がある旨の通知を受けたとき、または自らこれらのトラブルを検知したときは、必要な対処をとるものとする。

③ トラブル発生時の報告

トラブル発生時における発注者への報告の方法および対処に要する時間などは、協議の上決定するものとする。

⑸ 情報セキュリティ要件

システムの機密性、完全性、可用性を確保し、不正アクセスや情報漏えいなどのセキュリティリスクの低減を図る対策と要件を下記とする

① バックアップ対策

データ消失を防止するセキュリティ要件を表５に示す。

（表５）バックアップ対策

No	項目	目的
1	定期バックアップ	システム環境やデータベースの消失・破損に備え、迅速に復旧できるように定期的にバックアップを取得する。
2	バックアップ保管場所	火災、地震、水害などの災害や盗難のリスクを考慮し、バックアップデータを安全な場所に保管する。保管場所 は、システムの稼働環境とは異なるサイトとし、災害や事故による同時消失に備える。
3	バックアップ体制の確立	バックアップ作業の手順書を作成し、担当者を明確にすることで、復旧作業の確実性を向上させる。また、定期的にバックアップデータの復元テストを実施することで、データの完全性と可用性を検証する。

② 脆弱性対策

セキュリティの脆弱性による情報漏洩や不正アクセスを防止するセキュリティ要件を表６に示す。

（表６）脆弱性対策

No	項目	目的
1	脆弱性診断	システムの脆弱性を定期的に診断し、発見された脆弱性を速やかに修正することで、セキュリティリスクを低減し、システムの安全性を維持する。

③　不正アクセス防止対策

不正アクセスを防止するセキュリティ要件を表７に示す。

（表７）不正アクセス対策

No	項目	目的
1	ID/パスワード	ID とパスワードによるアクセス認証を実施する。
2	アクセス制御	アクセス権を設定し、不要なアクセスを制限する。
3	ファイアウォールの設置	外部からの不正アクセスを遮断するため、ファイアウォールを導入し、許可されていない通信を制限する。
4	サーバの隠蔽	サーバがインターネットから直接アクセスできないよう、DMZ（非武装地帯）にリバースプロキシサーバを配置し、サーバへの直接的な攻撃を遮断する。

④　物理的なセキュリティ対策

システムを収容する施設に対する災害・不正侵入・環境変化によるトラブルを防止するセキュリティ要件を表８に示す。

（表８）物理的なセキュリティ対策

No	項目	目的
1	データセンターの活用	信頼性の高いデータセンターを利用することで、堅牢な施設セキュリティ、24 時間 365 日の監視体制、安定した電力供給、適切な温度・湿度管理などの環境対策を実現し、サーバへの物理的な脅威を排除し、システムの安定稼働を確保する。

⑤　暗号化通信対策

通信内容の盗聴や改ざんを防止するセキュリティ要件を表９に示す。

（表９）暗号化通信対策

No	項目	目的
1	SSL/TLS通信	インターネット上での通信内容を暗号化し、第三者による盗聴や改ざんを防ぐ。
2	証明書の管理	SSL/TLS証明書の有効期限切れによるセキュリティリスクを回避するため、証明書の有効期限を適切に管理し、期限切れ前に更新する。

⑥　運用保守要件

システムの安定稼働と効率的な運用・保守を行うための運用保守要件を表１０に示す。

（表１０）運用保守要件

No	項目	目的
1	データ管理計画の策定	データのライフサイクル（収集、保存、利用、共有、廃棄）全体における管理方法を明確化し、データの品質、可用性、セキュリティを確保する。これにより、データの紛失や漏洩を防ぎ、適切なデータ活用を促進する。
2	運用計画の策定	システムの安定稼働と効率的な運用を確保するため、運用体制、運用手順、障害対応手順、保守計画などを明確 化し、システムのライフサイクル全体を通して最適な運用を実現する。
3	運用体制の構築	システムの安定稼働とセキュリティ確保のため、責任と役割を明確にした運用体制を構築し、効率的な運用と迅速な障害対応を実現する。
4	セキュリティ教育の実施	運用・保守に関わる者に対してセキュリティ意識向上を図り、情報セキュリティ事故の発生リスクを低減する。
5	定期メンテナンスの実施	サーバの過負荷や容量不足、ソフトウェアの不具合などを定期的に点検し、システムの安定稼働を維持する。また、セキュリティパッチの適用やソフトウェアのアップ デートを行うことで、セキュリティリスクを低減し、システムの信頼性を向上させる。

⑺　住宅地図ライセンス

草加市全域の住宅地図を取り扱う主要な地図提供会社として ZENRIN の住宅地図を支援システムのスマートフォンアプリケーション、苦情・事故受付、データ管理機能において取り込み、用いることとする。

①　契約プラン

ゼンリン住宅地図を利用、必要な機能を地図の描画と住所検索に限定し、利用者数は前述の人数（委託業者への地図配布可）とするプランを想定している。

ライセンス契約者以外の複製利用は行わないこととする。

詳細内容については契約後、発注者と協議し決定する。

⑻　データの最低保存期間

道路の維持管理とデータ分析の観点から、データの保存期間は１０年とする。

ただし、契約終了後のデータの取り扱いに関しては、６　基本事項 ⑸ システムサービス終了時のデータの取り扱いのとおりとする。

なお、データ抽出についてはシステム上にて Excel 出力により行うものとし、データに関する権利は市に帰属する。

⑼　道路維持管理システムの拡張性

システム導入後も、道路維持管理を取り巻く環境は、技術の進歩や新たな課題の発生などにより常に変化する。そのため、変化する業務環境に合わせて継続的な機能改良を実現できる拡張性を備えておく必要があり、導入後でも AI などの最新技術を搭載・連携可能なシステムとすること。また、他の情報システムとの連携が可能であることや、将来的に道路以外の分野への拡張が可能なシステムとすること。

⑽　システム利用率向上に対する提案

本システムによる要望受付において、誰もが簡単で楽に通報できると感じることができ、また、システム利用率において、電話及びメールによる通報の割合に対し、将来的にそれを超えることができるような工夫について検討し、提案すること。

8　その他

⑴　個人情報の保護に関する法律（平成１５年法律第５７号)、別記個人情報取扱特記事項及び別記外部委託における情報セキュリティ遵守事項を遵守すること。また、業務上知り得た事項を漏らしてはならない。

⑵　草加市環境マネジメントシステムに基づく取組に協力すること。

⑶　草加市政における公正な職務執行の確保に関する条例（平成１９年条例第１６号）第６条及び草加市が締結する契約からの暴力団排除措置要綱（平成８年告示第１５５号）第９条の規定に基づき、次の事項を遵守すること。

①　受注者及び受注者の下請業者が不当要求行為を受けた場合又は不当要求行為による被害を受けた場合若しくは被害が発生するおそれがある場合は、市長に報告するとともに、所轄の警察署に通報すること。

②　受注者は、市及び所轄の警察署と協力し、不当要求行為の排除対策を講じること。

⑷　仕様に疑義が生じた場合は、担当課と協議すること。

⑸　借上期間中に、本案件に係る法令等の制定及び改廃があった場合は、仕様書等の変更によることなく、その内容を遵守すること。

⑹　業務の実施に当たっては、人権を尊重するとともに、業務に関わる者が人権に配慮することができるよう努めること。

9　問合せ先

草加市役所　維持補修課補修係

電話０４８（９２２）２４１２（直通）

別記

個　人　情　報　取　扱　特　記　事　項

（基本事項）

第１条　この契約により、草加市（以下「発注者」という。）から事務の委託を受けた者（以下「受注者」という。）は、この契約による事務を処理するに当たり、個人情報を取り扱う際には、個人情報保護の重要性を認識し、個人の権利利益を侵害することのないようにしなければならない。

（秘密保持）

第２条　受注者は、この契約による事務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。

２　受注者は、この契約による事務に従事させる者に対し、在職中及び退職後においても、この契約による事務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないことその他個人情報の保護に関し必要な事項を周知しなければならない。

３　前２項の規定は、この契約が終了し、又は解除された後においても同様とする。

（作業場所の特定）

第３条　受注者は、発注者の指定した場所又は受注者の求めにより発注者が承認した場所以外で、個人情報を取り扱ってはならない。なお、発注者の承認は、書面でなければならない。

（厳重な保管及び搬送）

第４条　受注者は、この契約による事務に係る個人情報の漏えい、改ざん、毀損、滅失その他の事故を防止するため、次に掲げる事項を遵守し、個人情報の厳重な保管及び搬送に努めなければならない。

⑴　受注者は、発注者の許可なく、発注者の指定した場所又は発注者が承認した場所から個人情報又は個人情報を含む契約目的物等（以下「個人情報等」という。）を持ち出してはならない。

⑵　受注者は、個人情報等を発注者から受けるとき又は発注者に渡すときは、個人情報の内容、数量、受渡し日、受渡し確認者その他必要な事項を記載した書面を発注者と取り交わさなければならない。

（再委託の禁止）

第５条　受注者は、発注者の承諾があるときを除き、この契約による事務に係る個人情報の処理を自ら行うものとし、第三者にその処理を委託してはならない。

（委託目的以外の使用等の禁止）

第６条　受注者は、発注者の指示又は承諾があるときを除き、この契約による事務に係る個人情報を当該事務の処理以外の目的に使用し、又は第三者に提供してはならない。

（複写及び複製の禁止）

第７条　受注者は、発注者の指示又は承諾があるときを除き、この契約による事務に係る個人情報を複写し、又は複製してはならない。

（事故発生時の報告義務）

第８条　受注者は、個人情報の個人情報取扱特記事項に違反する事態が生じ、又は生じるおそれがあることを知ったときは、速やかに発注者に報告し、その指示に従わなければならない。この契約が終了し、又は解除された後においても同様とする。

（個人情報の返還又は処分）

第９条　受注者は、この契約が終了し、又は解除されたときは、この契約による事務に係る

個人情報を速やかに発注者に返却し、又は漏えいを来さない方法で確実に処分しなければならない。

（措置事項に違反した場合の契約解除及び損害賠償）

第１０条　発注者は、受注者がこの個人情報取扱特記事項に違反していると認めたときは、契約の解除及び損害賠償の請求をすることができる。

（個人情報の取扱い状況に係る検査）

第１１条　受注者は、年間１回以上、個人情報取扱特記事項遵守状況確認報告書を、第３条の規定により承認を受けた場所、第４条の規定により個人情報を保管している場所、個人情報の管理に関する責任者及び業務従事者の管理体制及び実施体制その他の個人情報の管理の状況がわかる資料とともに発注者に提出することとする。発注者はその内容を精査し、必要があると認められるときは、受注者に対し、立入検査又は立入検査に相当する調査措置を講ずることができる。

（その他）

第１２条　受注者は、第２条から前条までに掲げるもののほか、個人情報の適正な管理のために必要な措置を講じなければならない。

別記

外部委託における情報セキュリティ遵守事項

基本事項

草加市は、保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策の基本的事項を「情報セキュリティ基本方針」として定めている。また、当該セキュリティ対策の有効性及び効率性の確保を目的として、遵守すべき行為、判断等に関する基本的事項を「情報セキュリティ対策基準」として定めている。

市の情報資産を取扱う業務の受注者は、当該基本方針及び対策基準の適用範囲に含まれることから、次の事項を遵守し、市の情報資産の機密性、完全性及び可用性を維持するよう努めなければならない。

情報の分類

受注者は、原則として次の分類を行った上で、情報を保護すること。

市保有情報	市から貸与された情報のこと。
重要情報	市から貸与された情報の内、個人情報、特定個人情報及び非公開情報を含む情報のこと。

情報の保護

受注者は、次の対策に努めること。

共通	市の承諾なしに、市保有情報の一部又は全部を第三者へ提供することのない制御すること。
市保有情報	市保有情報を取扱う作業従事者を明確にし、その範囲内でのみ取扱うよう制御すること。 市保有情報を保管する場所は、作業従事者のみが取扱えるよう制御すること。 契約満了時等で市保有情報を市へ返却する際は、受注者内にデータ等が残らないよう消去する手順が確立すること。 市保有情報を受注者のファイルサーバ等で電子データとして保有する場合、作業従事者のみがアクセスできるよう制御すること。 市保有情報を作業従事者が市に無断で持ち出すことがないよう管理を徹底すること。 市保有情報を市と電子メールでやり取りする場合、暗号化等の情報漏えい対策を行った上でやり取りすること。 市保有情報を運搬することがある場合、盗難及び紛失対策を行った上でやり取りすること。
重要情報	【市保有情報における制限に加えて】 業務従事者のパソコンは、関係者以外からの覗き見防止等の対策を行うこと。 業務従事者がUSBメモリ等の電磁的記録媒体を使って不正に情報がコピーされることがないよう適切に制御すること。 業務従事者のパソコンは、OS等を最新の状態とすること。ただし、システムの動作検証のため、過去のOSを使用する必要があるなど、理由がある場合については、この限りでない。 業務従事者のパソコンは、盗難及び紛失時にデータが漏えいしないよう対策が施すこと。

ネットワークの強靭化対策

受注者は、重要情報を取扱う作業環境を様々な情報セキュリティリスクから保護しなければならない。また、特定個人情報を取扱う環境はインターネットから分離した環境を用意し、そこでのみ取扱うこと。その他、総務省が発行する「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（以下「総務省ガイドライン」という。）」で示された基準を遵守すること。

物理的セキュリティ

受注者は、原則として次の物理的対策を講じること。

管理区域	サーバ等の機器を設置する場所は、管理区域とし管理すること。 外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止すること。 管理区域への入室は、入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行うこと。 管理区域に入室する場合、身分証明書等を携帯し、求めにより提示すること。 当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないこと。
装置のセキュリティ	サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じること。 通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じること。 電磁的記録媒体を内蔵する機器を受注者以外に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、管理責任者は、外部の事業者に故障を修理させるにあたり、修理を行う事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行うこと。
通信回線・機器	ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らすこと。

人的セキュリティ

受注者は、業務従事者に対し必要な情報セキュリティ教育・トレーニングを行うこと。また、市の求めに応じてその実施記録の提示を行うこと。なお、業務従事者に対し、異動、退職等により業務を離れる場合には、利用していた機器等を返却させるとともに、その後も業務上知り得た情報を漏らしてはならない旨を合意させること。

技術的セキュリティ

受注者は、次の情報セキュリティ対策を行うこと。

アクセス制御	原則として、情報システム及びパソコンを使用する際は、業務従事者ごとにIDを発行すること。 業務従事者のIDは、本人以外がアクセスできないよう認証方法は最良の方法を選択すること。
開発・導入	開発で用いる環境に対して、管理責任者の管理の元で適切な対策を行うこと。 システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発

	用IDを削除すること。 システム開発、保守及びテスト環境とシステム運用環境を分離すること。 重要情報を、テストデータに使用しないこと。
不正プログラム対策	業務従事者が操作するパソコン等は、コンピュータウイルス等の不正プログラム対策ソフトウェアを導入し、パソコン等に常駐させること。 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。
不正アクセス対策	外部からの不正アクセス及び内部不正に備え、情報漏えいを防止するために必要な対策を講じること。 不正通信、不正操作等を牽制するための必要な監視を行うこと。

監査等への協力

受注者は、市の求めに応じて立入検査等に応じること。

その他

受注者は、上記以外の基準が必要となった場合は、総務省ガイドラインを参照するとともに、市と協議し対策を行うこと。

以　上