

令和8年度
防犯アプリ運用事業
仕様書

令和8年4月
宮城県警察本部

防犯アプリ運用事業仕様書

1 委託業務名

防犯アプリ運用事業

2 委託業務の目的

スマートフォンアプリ（以下「アプリ」という。）を用いて県民の安全対策に必要な地域における犯罪発生情報、特殊詐欺関連情報、不審者情報等を、県民に対してタイムリーに、かつ、分かりやすく発信し、県民の防犯意識の高揚と自主防犯活動の活性化を促すことにより、防犯力を高め、もって、安全・安心な地域社会を実現することを目的とする。

3 契約期間

契約締結の日から令和9年3月31日まで

4 委託業務の履行期間

(1) 開発

契約締結日から令和8年12月31日まで

(2) 運用管理・保守

令和9年1月1日から令和9年3月31日まで

5 委託業務の内容

(1) アプリの設計・開発

(2) プロジェクトの管理

(3) アプリのテスト

(4) アプリの公開

(5) 管理者研修

(6) 運用管理・保守

(7) 指定するドキュメントの作成

(8) 上記(1)から(7)までの附帯業務

6 一般事項

(1) アプリを構成するソフトウェア、ライセンス等について、本仕様書に記載がないものであっても、アプリの機能を実現するために必要なものは、本契約に含めること。

(2) 開発及び保守体制について、防犯アプリ運用事業企画提案募集要領に示す期日（閉庁日を除く。）までに、別記様式「提案機器等一覧」及び説明資料を宮城県警察本部（以下「発注者」という。）に提出、説明し、承認を得ること。承認が得られなかった機器等については、代替えの機器等を提示し、あらためて説明の上、承認を得なければならない。この場合において入札までに承認が得られなか

ったときは、入札に参加できないものとする。

- (3) 契約期間終了後の情報の抹消費用を含めること。
- (4) 本仕様書に定めのない事項又はアプリの開発にあたって疑義や支障が生じた場合は、その都度発注者と協議し、その指示に従うこと。

7 報告・打合せ・連絡手段等

- (1) 本業務開始に当たり、委託業務着手報告書（別記様式第1号）により、生活安全企画課長を通じて発注者に報告すること。
- (2) 定期的及び作業の区切りに進捗状況を任意様式により発注者に報告すること。
- (3) アプリの開発業務の進捗、品質等の問題点については、速やかに発注者に報告し、その対応を協議した上で、発注者の承認を経て以降の業務にあたること。
- (4) 発注者が随時の打合せを要求した場合、これに応じること。
- (5) 打合せに必要な資料は、発注者の要求に従い受注者にて作成すること。
- (6) 受注者が発注者に資料を要求する場合は必ず書面をもって行うこと。
- (7) 受注者は打合せ後に議事録を作成し、発注者の承認後、双方で保管すること。
- (8) 使用方法、運用方法等に関する説明、質問、相談等に応じること。
- (9) 全ての業務が完了したときは、委託業務完了報告書（別記様式第2号）により、生活安全企画課長を通じて発注者に報告すること。

8 特記事項

- (1) 発注者がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合は、発注者と迅速かつ密接に連携し、代替品選定等を行うこと。
- (2) 不正な変更（機器等の製造工程、流通過程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことをいう。）が疑われると発注者が判断した場合は、受注者の責任のもとで調査及び必要な措置を講ずること。

9 仕様等

(1) アプリ

別紙1「機能要件」のとおり

(2) 設計・開発

ア 要件確認

(ア) 機能要件を発注者と協議して確認・整理を行うこと。

(イ) 外部連携に関するインターフェース等の要件については、発注者及び関係者と調整して決定すること。

イ 基本設計

(ア) 提供する機能及びシステム方式、画面遷移の概要、画面のデザイン等を設計すること。

(イ) システム構築設計書（基本設計書）を作成し、発注者の承認を受けること。

ウ 詳細設計

基本設計を基に、実装する機能の主要な設計項目について、詳細設計書を作

成すること。

エ 開発

詳細設計を基に、プログラム製造及びプログラム単体でのテストを行い、構成・変更管理を行うこと。

オ 意見の反映

開発に当たっては、宮城県警察の各部署が集約した、機能等に係る意見に基づいて開発を行うこと。

(3) プロジェクトの管理

ア アプリの開発プロジェクトを管理するため、受注者は開発責任者を定めること。

イ 受注者は、設計・開発工程におけるスケジュール、成果物、役割分担及びプロジェクトの管理方法を記した作業計画書を作成すること。

併せて、プロジェクトの責任者、人員等を記した作業体制図を作成し、警察本部の承認を受けること。

ウ 受注者は、承認された作業計画書及び作業体制図に基づき、設計・開発業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行い、プロジェクトを管理すること。

エ 受注者は、承認された作業計画書及び作業体制図に基づき、プロジェクトの進捗状況報告書を作成し、必要に応じて発注者に報告すること。

(4) アプリのテスト

アプリのテストは、総合テスト、試行運用テストを行うものとする。

テストの実施に際しては、事前にテスト計画書を作成し、発注者に提出した上で、テストを実施すること。

テスト終了時に、実施内容、品質評価結果、及び次工程への申し送り事項等について、テスト結果報告書を作成し、発注者に報告の上、承認を得ること。

ア 総合テスト

アプリが基本設計の仕様を満たしていることを確認するために総合テストを行い、システムが納品可能な状態であることを確認すること。

確認に当たっては、ソフトウェア製品が仕様に適合し、かつ実稼働環境で利用可能であることを確認できる評価指標又は合格条件を設定した上で、必ず実機を用いて実稼働環境と同等の環境において総合テストを実施すること。

この際には、性能や可用性に係るテストも実施すること。

イ 試行運用テスト

総合テスト実施後、アプリ公開前までの間、発注者が指定する者に検証用のアプリを提供すること。

なお、アプリ公開時には検証用アプリは消去するものとする。

(5) アプリの公開

開発したアプリは各スマートフォンアプリストアにて無償公開すること。

また、アプリストアへの登録申請から公開までの手続きについて、発注者が行

わなければならない手続きの補助または必要な代行作業を受注者が行うものとする。

登録審査に問題が生じた場合は、アプリの仕様修正を含め、発注者と改めて協議を行うものとする。

公開の際、公開者が「宮城県警察」であることを、明確に示すこと。

(6) 管理者研修

操作マニュアル、研修資料を作成・提供すること。

また、管理者機能の操作方法等の研修を、試行運用テスト開始時及び発注者の要請に応じて、発注者における対面研修またはWeb等による非対面方式などにより1回以上実施すること。

(7) 運用管理・保守

ア 運用管理

(ア) 受注者は、アプリの運用が常時正常な状態で利用できるような体制を整備すること。

(イ) アプリの運用において障害が発生した場合、障害原因を究明し、障害を復旧させる手段を講じること。また、障害原因等を書面で発注者に報告すること。

(ウ) サポート窓口は一本化し、休日以外の日（以下「平日」という。）の午前9時00分から午後5時00分までの間、発注者からの電話又は電子メールを受け付ける窓口を設けること。

(エ) 平日午前9時00分から午後5時00分までの間で、発注者が保守員の派遣を必要と判断した場合、受注者は速やかに必要な知識及び技術を有する保守要員が保守環境に対して直接対応に当たることのできる体制を整備すること。

(オ) OSのバージョンアップは無償で対応すること。

機能の追加や改修の必要がある場合は、発注者と協議すること。

(カ) 保守作業を実施する場合は、事前に保守作業の内容を発注者に提示して、承認を得ること。

(キ) 契約期間の満了時には、受注者が保存しているデータを消去するなどの措置を行い、発注者に結果を報告すること。

(ク) 利用者数等に関するレポートを作成し、月1回発注者へ報告すること。

ただし、受注者が使用する管理画面等で確認できる場合はレポートの作成は不要とする。

イ データセンター

(ア) アプリに関するデータの管理のためのデータセンターを設置すること。

データセンターは24時間365日体制の監視、運用体制を要していること。

ただし、事前協議があり、かつ通常必要と認められるメンテナンス等に係る停止は除く。

(イ) サーバは、日本国内のデータセンターにおいて、運営管理等の全てが行われていること。

(ウ) データセンターの設備

- a 常時施錠するとともに、立入りを許可されていない者が立ち入らないように、立ち入る者が許可された者か否かを確認できるような措置をとること。
 - b ICカード、生体認証など、入退室に係るセキュリティ対策を要していること。
 - c ISMS（情報セキュリティマネジメントシステム）基準に則したコンピュータ専用ビルであること。
 - d 地震・火災・電源・漏水・防犯監視・データ保管対策が十分とられていること。
 - e 地震対策にあつては、建築基準法の耐震基準を満たした建物で、震度7クラスの地震発生時にもサービス提供可能な耐震、免震又は制震構造であること。
 - f 火災対策にあつては、全館防火壁、不活性ガス消火設備などを装備していること。
- ウ 停電対策にあつては、二系統受電設備、UPS（400KVA相当以上）、専用発電機（1000KVM相当以上）を設備していること。
- エ 浸水・漏水対策にあつては、漏水検知機、防水堤等を装備していること。
- オ 防犯対策にあつては、ガラス損傷警報装置（電算機室は鉄板による無窓化）、専用カード入退室管理装置、血流入退室管理装置、各種防犯センサー、監視カメラ等を装備していること。
- カ 機密保持対策にあつては、耐火仕様専用データ保管庫等を装備していること。
- (8) サーバ・通信設備の運用
- ア サーバ機器の多重化、無停電装置の設備等、安定運用のために万全の対策を講じていること。
- イ サーバの設置場所は、常時適切な温度・湿度で管理されていること。
- ウ 通信設備及びハードウェアの冗長化が行われ、レスポンスに配慮した分散処理が可能であること。
- エ ファイアウォールによる防御措置及び不正アクセスを防御するシステムが設置されていること。
- オ 不正プログラム対策ソフトウェアの導入及び最新のパターンファイルの適用並びに定期的な不正プログラム検査を実施すること。
- また、ウイルス対策を施し、常に最新のパターンファイルを保っていること。
- カ 障害時の対応方法が明確にされており早急な対応が可能であること。
- キ セキュリティホールを解消するためにOSのパッチ適用等必要な対応を行っていること。
- ク 不正アクセス、異常アクセス等に対応するアクセス監視対策が整備されていること。
- ケ データ更新等のための通信回線やサーバのアクセスに、十分なセキュリティが確保されていること。
- コ 発注者以外の者が情報登録したデータの改変、閲覧、取得ができない対策を、

ID・パスワード以外の方法においても講じること。

サ 受注者は、ISO9001、ISO/IEC27001（又は「JIS Q 27001」）を取得している者とし、十分な個人情報保護の対策を講じていること。

シ セキュリティ対策を常に行い、機能を保全すること。ただし、何らかの被害があった場合に備え、機能停止手段を準備しておくこと。

ス システム障害や不正アクセス等のセキュリティ侵害事案を認知した場合は、発注者に通知すること。

セ 不正アクセス等のセキュリティ侵害対策のため、常に発注者と協力すること。

(9) 運用条件

ア 著作権等のある地図等を使用する場合は、不特定多数の利用者が利用するための権利を取得すること。

イ 利用者に快適なサービスを提供できるよう機器・通信回線等を選定すること。

ウ アプリには、発注者が指示したサイト以外へのリンク、広告及び発注者を判別することが可能なロゴ等の掲載は行わないこと。

エ 運用開始後においても表示項目及び項目の増減について、柔軟な対応を可能とすること。

オ iOS、Androidのバージョンアップに伴う動作検証を行うとともに、必要な場合は修正バージョンを作成すること。

カ アプリの利用画面は使い方が分かりやすく、簡単であること。

また、誤操作等を防止するデザインであること。

キ 利用者のスマートフォンには、発注者が提供するアプリ以外のアプリをダウンロードさせる必要がないこと。ただし、汎用的なドキュメントビューア等、別に必要と思われるアプリがある場合には、発注者と協議すること。

ク 本サービスに搭載されるコンテンツの著作権、その他の知的財産権は、従前から受注者又は第三者に帰属するものを除き、発注者に帰属する。

ケ 本サービスの提供を目的としてデータセンターに設置されたサーバ等の機器の所有権及び本サービスを構成するサーバに関するプログラムの著作権等の知的財産権は、受注者及び受注者に利用許諾する第三者に帰属する。

コ 本サービス向けに提供されるASPサービスの機能については、他者及び他人が保有する基本的特許及び周辺特許に抵触しないものとする。

サ 受注者は業務の履行で知り得た事項を、第三者に漏らしてはならない。また、データの秘密保持については、万全の管理を行うこと。

シ 機器更新などによるサービスの運用停止は認めない。ただし、やむを得ない場合には次の措置をとること。

(ア) 計画的停止

受注者は、保守上の理由からサービスの運用を計画的に停止する場合には、2週間前（ただし、セキュリティ上の理由で、早急な対応が必要な場合はその限りでない）までには、発注者に報告すること。

なお、当該停止により発注者に支障が生ずるときには、停止期間の変更等について協議すること。

(イ) 非常停止

受注者は、天変地異等の非常事態その他、受注者の責めに帰することができない事由からやむを得ず本サービスの運用を一時停止する場合、速やかに発注者に報告すること。

(ロ) 保証等

ア システムの障害等による異常を発注者が認知した場合は、発注者の通知により、受注者の責任と費用負担により速やかに必要な修理、調整を行い、発注者に経緯等を報告するものとする。

イ 稼働後におけるソフトウェア等の契約不適合によるシステム不具合が発生した場合は、受注者の責任と費用負担により速やかに不具合を収束させ、発注者に報告するものとする。

10 サービスレベル要件

下表のサービス品質基準をもとに、必要な項目及び詳細な事項（ペナルティ含む。）を発注者と協議して、運用開始日（令和9年1月1日）までにサービスレベル協定（以下「SLA」という。）を締結すること。

(1) SLAの見直し

本システム稼働直後6か月間は検証初期運用期間として、サービスレベルの測定を行った上で、受注者と協議を行い、SLAの見直しを行うこと。

(2) SLAの測定

SLAの測定サービスレベルの測定は月ごとに行うこと。

(3) サービスレベル管理結果対応

サービスレベルが未達成の場合の措置として、受注者は業務への影響や緊急性等の度合いに応じ、暫定的及び中期的に必要な措置を提案及び実施すること。

サービスレベル項目		基準値
システム可用性	サービス時間	24時間365日（計画停止は除く）
	稼働率	99.9%以上
	計画停止	1%未満（1回の停止は8時間以内）
サービスサポート（運用保守）	質疑・保守要請受付時間	平日の9時00分から17時00分まで
	障害受付時間	24時間365日
	障害保守サービス	24時間365日
	障害対応	95%が2時間以内に対応を開始すること。 最大でも12時間以内に対応を開始すること。
	定期点検保守作業	半年に1回
	定期報告	月に1回
	ハードウェア障害対応	可用性 ウイルスを検知してから通知するまでの時間が15分以内

		確実性	不正アクセスを感知してから通知するまでの時間が15分以内
セキュリティサービス	ウイルス対策		ハードウェアが故障している時間の比率0.5%以下
	ファイアウォール		障害発生から障害復旧までの時間が3時間以内
ネットワークサービス	回線通信	可用性	故障により停止している時間の比率が0.1%以下
	帯域確保機能	性能	あり
	障害管理	確実性	異常を検出し、復旧するまでの時間3時間以内

11 情報セキュリティ要件

受注者は、本業務の履行に当たり、別紙2「情報セキュリティの確保に関する特約条項」を遵守するものとする。

12 アプリケーション・コンテンツについて

- (1) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。
- (2) 提供するアプリケーション・コンテンツが脆弱性を含まないこと。
- (3) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
- (4) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。
- (5) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないように、アプリケーション・コンテンツの提供方式を定めて開発すること。
- (6) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないように開発すること。

13 納品成果物

	成果物	納品期限
ア	作業計画書・導入体制表	契約締結後速やかに
イ	システム構築設計書（構成図を含む）詳細設計書	要件確認後速やかに
ウ	テスト計画書	適宜テスト実施前
エ	テスト結果報告書	適宜テスト実施後速やかに
オ	操作マニュアル、研修資料	令和8年12月31日
カ	障害対応連絡先・体制図	令和8年12月31日
キ	作業員名簿	契約締結後速やかに
ク	システム運用計画書	令和8年12月31日

ケ	障害対応連絡先・体制図	令和8年12月31日
コ	システムアプリケーション	令和8年12月31日
サ	納品一覧表	令和8年12月31日

14 納入場所

納品成果物は、発注者が指定する場所。

15 納入方法

DVD-ROM等電磁的記録媒体に格納したもの（原則、Microsoft Officeで作成するものとする。）により納品すること。

なお、操作マニュアル・研修資料については、紙媒体で2部納品すること。

16 納入期限

令和8年12月31日までに提出すること。

17 知的財産権の帰属等

(1) 本契約の作業により作成する発注者独自の成果物に関し、著作権法に関し、著作権法（昭和45年法律第48号）第21条、第23条、第26条の3、第27条及び第28条に定める権利を含む全ての著作物を発注者に譲渡し、発注者は独占的に使用するものとする。

(2) 成果物に第三者が権利を有する著作物が含まれている時は、発注者が特に使用を指示した場合を除き、受注者は当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。

なお、この時、受注者は当該著作権者の使用許諾条件につき、発注者の了承を得るものとする。

18 その他

(1) 受注者は、受注業務の遂行に及び日本国において定められた法令を遵守すること。

(2) 本仕様書に定めのない事項等については、発注者と受注者で協議のうえ決定するものとする。

別紙1 機能要件

1 アプリ全般について

(1) アプリの概要

ア 地図情報を基本メニューとした各種機能を提供するものであること。

イ 基本メニューのうち、一部の情報をプッシュ通知により利用者に通知する機能を有すること。

ウ Android及びiOS対応のスマートフォン端末で、OSはAndroidOS13.0以降、iOS16以降に対応すること。ただし、開発時期等によってはOSのバージョンは変更する場合もある。

エ 詳細な住所地、氏名、電話番号の登録が不要な仕様であること。

オ サーバに位置情報を連続的に蓄積しない仕様であること。

(2) ダウンロード及びインストール

ア 利用者がAndroid及びiOS対応スマートフォン向けのアプリケーションダウンロードサイト（Google Play Store及びApp Store）から無償でダウンロードできるようにすること。

また、各アプリストアへの登録申請から公開までの手続きについては、受託者の費用負担により行い、手続きの補助または必要な代行作業を受注者が行うこと。

イ ダウンロードの際、各アプリケーションストアから全ての機能を一括してダウンロードし、インストールできるようにすること。

(3) 各種設定機能

ア インストール後の初期登録設定

登録設定は、利用者がいつでも登録内容を修正・再登録できるものにする事と。

(ア) 利用者登録

○ 利用者の属性に関する項目をリストから選択できること。

項目内容については、別途宮城県警察本部（以下「警察本部」という。）と協議するものとする。

○ 利用者登録は、利用者の属性分析に資することを目的とし、目的と任意登録であることを必ず明示すること。

(イ) プッシュ通知設定登録

○ 通知を受信する市町村、住まいを管轄する警察署等を複数選択できること。

○ 通知を受信する属性を選択できること。

(ロ) 防犯ブザー・痴漢対策機能の設定

○ 警報音の大きさ及び作動条件を設定できること。

○ メールを送信先又はプッシュ通知の通知先等を複数選択できるようにすること。

なお、メールアドレス等についてはサーバに格納しない仕様とすること。

- 名同時の通知先を3件まで登録できること。
- 注意事項を表示し、同意後に各種設定ができること。
- (エ) 現在地の送信機能登録
メールの送信先又はプッシュ通知の通知先等を複数選択できるようにすること。

2 アプリ機能

(1) 地図情報機能

ア 概要

「犯罪情報」、「特殊詐欺予兆電話情報」、「不審者情報」等で構成し、それぞれの情報を表示すること。

なお、地図情報が7種類まで増やせる想定でリソースを事前に確保しておくこと。

イ 表示項目

(ア) 各種情報の地図表示

- a 町名区域（町丁目単位）を着色してエリア表示すること。
- b 着色した区域をタップすると、属性情報を表示すること。
- c GPS機能を連動させて利用者の現在地をアイコンで表示し、利用者が一目で識別できるようにすること。
- d 各種情報のアイコン等を設定し、当該アイコン等をタップすることでマップを自由に切替え及び重ね合わせられるようにすること。
- e 情報の種類・数・表示色・表示期間等については、別途宮城県警察との協議とする。

(イ) 警察施設

発注者が指定した警察施設をアイコンで表示し、押下することで属性情報（警察情報、所在地）を表示すること。

(ロ) 地図情報の表示

地図情報は、各地図情報の切替え及び重ね合わせ表示に対応すること。

(ハ) 背景地図

- a 必要なライセンスは受注者が用意すること。
- b 背景地図の更新は、システムを止めることなく、最新の背景地図データを提供すること。
- c 運用開始後の背景地図に関する費用も受注者の負担とする。

(ニ) 基本操作性

- a 地図のスクロールや拡大・縮小は、表示が途切れることなくスムーズに連続して動作できること。
- b 縮尺に応じて、地図上の図柄や注記等の表示項目が自動的に見やすくなるように調整されること。
- c タッチスクリーン操作に最適化すること。

(ホ) 付近情報の自動表示

地図の表示範囲に合わせて、画面下部に発生情報を、自動で絞り込み表示すること。

(キ) ルート検索

現在地から近い警察署や交番へのルートを検索すること。

(ク) 情報共有

地図に配信された情報について、利用者がメール、LINE、X（旧Twitter）等を使用して素早く共有できること。

(ケ) その他

a 情報のアイコンは、運用開始後でも変更できること。

b 操作方法の説明画面を設置すること。

(2) 防犯ブザー機能

ア 概要

利用者が不審者又は犯罪被害に遭遇するなど、身に危険を感じたとき、警告音の吹鳴等、周囲に危険を知らせることができる機能を有すること。

イ 基本仕様

(ア) 機能起動時に、一定条件の動作により作動・停止する機能を用意すること。

(イ) ブザー起動の条件となる動作は、緊急時も容易であるとともに、誤作動を極力避ける仕組みとすること。

(ウ) 110番通報もできるように、通話発信用のアイコン等を設置すること。

(エ) 機能を使用した際に、あらかじめ利用者が設定した通知先に、機能を使用した位置情報等をプッシュ通知で通知すること。

(オ) プッシュ通知の送受信について、履歴画面から通知内容を確認できること。

(カ) 複数のアイコン等により、機能を使用した際にブザー音が吹鳴するものとブザー音が吹鳴しないものの使い分けができること。

(3) 痴漢対策機能

ア 概要

利用者が、画面表示や警告音等で痴漢被害を未然に防止又は周囲に知らせる機能をつけること。

イ 基本仕様

(ア) 機能起動時に、一定条件の動作により作動・停止する機能を用意すること。

(イ) 機能起動の条件となる動作は、緊急時も容易であるとともに、誤作動を極力避ける仕組みとすること。

(ウ) 110番通報もできるように通話発信用のアイコン等を設置すること。

(エ) 犯人に警告する場合や周囲に知らせる場合等、状況に応じた複数の画面表示を用意すること。

(オ) 機能を使用した際に、あらかじめ利用者が設定した通知先に、機能を使用した位置情報等をプッシュ通知で通知できること。

(カ) プッシュ通知の送受信について、履歴画面から通知内容を確認できること。

(4) プッシュ通知機能

ア 概要

管理者機能から情報を入力し、利用者のスマートフォンにプッシュ通知できること。

イ 基本仕様

(ア) プッシュ通知を配信する際は、通知があったことをスマートフォン画面にダイアログを表示する、ツールバーにアイコンを表示するなど、利用者が一目で識別できるようにすること。

(イ) 情報配信と同時にプッシュ通知を行うこと。

(5) メール連携機能

ア 概要

みやぎSecurityメールから配信されたメッセージをアプリと自動連動し、アプリ利用者へ配信が可能なこと。

イ 基本仕様

(ア) カテゴリ毎の一覧表示で確認可能なこと。また、一覧から事案を表示した際に合わせて地図も表示すること。

(イ) 情報配信と同時に該当エリアに対してプッシュ通知を行うこと。

(6) ソーシャルメディア（SNS）及び宮城県警察ホームページ等連携機能

ア 概要

宮城県警察が公式アカウントを取得しているソーシャルメディア及び宮城県警察公式ホームページと連携し、アプリ上で表示すること。

イ 基本仕様

(ア) 現時点対象とするのは、「X（旧Twitter）」及び「YouTube」、宮城県警察ホームページとする。

(イ) 他のソーシャルメディア等と連携（リンクを含む）できる拡張性も有すること。

(7) 現在地の送信機能

ア 概要

アプリ内で利用者同士のグループを作成し、そのメンバー間のみメッセージや位置情報を共有する機能を提供すること。

イ 詳細

(ア) メンバー登録

a メンバー追加ボタンを押下することでQRコードが表示され、互いに読み取ることでグループ登録できること。

b 電子メールで招待できるURLを送信できること。

(イ) メッセージ配信機能

a メンバー一覧が表示され、チェックボックスで選択することで対象者にメッセージが送信できること

b メッセージは定型文とし、複数の定型文の中から利用者が選択できること。

(ウ) 位置情報共有機能

メッセージ発信時にメッセージとともに発信者の位置情報（現在地）が伝

達可能であること。

(8) エリア通知機能

管理者が定める特定のエリアに利用者が入った際に、管理者が作成した緊急情報やお知らせ等を、各OSの制約の範囲内でプッシュ通知として受信できること。

(9) お知らせ機能

ア 概要

地図に表示することが困難な情報を掲載できること。

また、利用者の登録設定に応じてプッシュ通知方式で情報を通知できること。

イ 基本要件

(ア) トップページに最新情報（5件程度）のタイトルを表示させ、各タイトルをタップすると詳細が表示されること。

(イ) 「詳しく見る」などのボタンを配置し、タップすると情報一覧画面が表示されること。

(ウ) 一覧から選択することで詳細情報が表示されること。

(エ) 各情報ページは、テキスト及び画像データ、各情報元のパソコン向けサイト等コンテンツへのリンクを表示できること。

(10) その他

管理者が容易にコンテンツ（コンテンツタグ）を上限無く追加できる仕組みとすること。

3 管理者機能（情報登録用インターフェース）

(1) データの管理（入力・修正・削除等）

ア データの管理はWebブラウザを用いることとし、受注者が提供する管理サイト上で行うことができること。

イ データの公開は発注者が用意するCSVデータを使用して行うが、これらのデータを取り込み、公開に適した形式に編集してCSVデータとして出力するアプリケーションを提供すること。

ウ 地図情報の表示については、編集後のCSVデータを取り込んで一括処理できる仕組みを用意すること。

エ 公開の際、CSVデータ内の住所情報から管理サイト上に地点等を表示させるとともに、発注者より、地点、属性情報等の修正ができること。

オ 運用中のデータ更新作業は、発注者で実施することが可能であること。

カ 動作環境は、Windows11以上とする。

なお、契約時点におけるOSのサポート期間等により、対応OS等の動作環境は変更する場合がある。

(2) 管理サイトへのアクセス及びログイン方法

ア 通信手段には、TLS、IPsec等による暗号化を行うこと。

イ 管理サイトへのログインは、ユーザID及びパスワードによる認証方式とし、複数のID及びパスワードを設定できること。

ウ 管理サイトへのアクセス方式が、発注者で使用中の動作環境以外のものが必

要な場合は、アクセスするための機器一式を用意すること。

エ 管理サイトへのアクセスは宮城県警察本部等特定の I P アドレスのみアクセス可能とすること。

なお、アカウントロックの設定及びアカウントロック解除の設定を可能な仕様とすること。

(3) ログインユーザの設定

ア ログインユーザのアカウント設定は、100件を上限に設定できること。

イ 発注者において、ユーザ単位でアカウント及び権限の設定をできるものとし、それぞれにユーザ I D 及びパスワードが設定可能であること。

(4) 更新されたデータの反映時期

更新（入力・修正・削除等）データは、速やかに反映されていること。

(5) 情報掲載件数

毎月の情報掲載件数は無制限とする。

また、サービス運用開始時点の搭載データは過去 5 年分とする。

(6) 地図機能のデータ管理

ア 発注者が別に保有する公開用データが、登録・修正・削除が可能であること。

イ データの更新は、管理者サイト上の管理メニューから行えること。

なお、地図の情報更新は、更新が一括反映される仕組みを提供すると。

(7) お知らせ機能

ア 管理者サイト上の「宮城県警察からのお知らせ」管理メニューにより行うものとする。

イ 新規に更新されたデータを識別するためのアイコン等を表示すること。

ウ データの更新は、別途発注者が指示するものとする。

エ データの更新は、管理者サイト上の業務メニューから行えること。

オ 登録状況、更新状況が一覧で確認できること。

(8) ログ解析

ア 管理者画面から、ログ情報を C S V データとして出力できること。

イ 各機能単位で、アクセス数や不具合発生状況を確認できること。

ウ 利用者登録の統計が確認できること。

エ アプリのダウンロード件数を O S 別で確認できること。

(9) データの返却

ア 契約満了後、発注者より受領したデータについては、複写物も含め全て発注者に返却すること。

イ データ返却に関しては、次期システムへの移行作業前に発注者と十分な協議を行うこと。

ウ データ返却の実施計画に関して過去の実績・ノウハウ等を最大限活用し、警察本部側担当者の作業負担が最小限となるような計画を立てること。

エ 事前に、返却に係るスケジュールを提出し、発注者の承認を得ること。

別紙 2

情報セキュリティの確保に関する特約条項

(目的)

第1条 受注者は、本契約に係る業務（以下「本件業務」という。）の実施のために、発注者から提供する情報その他本件業務の実施において知り得た情報（以下「保護すべき情報」という。）の機密性、完全性及び可用性を維持すること（以下、「情報セキュリティ」という。）に関して、この特約条項に定めるところにより、その万全を期さなければならない。

2 保護すべき情報の範囲は、次の各号とする。

- 一 発注者が秘密区分の指定をした秘密に属する文書、図面、図書等（電磁的記録を含む。）
- 二 発注者が秘密区分の指定をした秘密に属する物件
- 三 一又は二に掲げるものを基に、受注者が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件のうち、発注者が指定したもの
- 四 前各号について推知し得る情報

(再委託の禁止)

第2条 受注者は、本契約の全部又は一部を第三者に再委託してはならない。ただし、やむを得ず再委託（再々委託以降の委託を含む。以下同じ。）を行う場合は、あらかじめ再委託者の商号又は名称及び住所並びに再委託する業務の範囲、再委託の必要性、再委託期間、再委託率その他の情報セキュリティの確保に係る契約内容等を記した書面（以下「再委託承認申請書等」という。）を提出し、発注者の承認を得るものとする。

なお、再委託承認申請書等に記載された事項について、変更がある場合には、受注者はあらかじめ変更の届出を発注者に提出し、同様に承認を得るものとする。

- 2 前項ただし書により受注者が再委託を行う場合、受注者は受注者と再委託者との間で締結する契約において、再委託者において本特約条項と同等の情報セキュリティの確保が行われるよう定めなければならない。
- 3 発注者は、前項の契約について、再委託承認申請書等を確認し、再委託を行う合理的理由及び再委託者が再委託される業務を履行する能力その他の情報セキュリティの確保のために必要と認められる事項が十分満たされていないと認められる場合、第1項の承認を行わないことができる。
- 4 第1項ただし書により受注者が再委託させる場合の再委託者その他本契約の履行に係る作業に従事する受注者以外の事業者（以下「再委託者等」という。）における情報セキュリティの確保について、受注者は本特約条項に従い、必要な通知、申請、確認等を行うものとする。

(情報セキュリティ確保のための体制等の整備)

第3条 受注者は、保護すべき情報に係る情報セキュリティを確保するために必要な体制を整備しなければならない。

2 受注者は、受注者の代表者又は代表者から代理権限を与えられた者を情報セキュリティに係る責任者（以下「情報セキュリティ責任者」という。）とし、情報セキュリティ責任者の下に、保護すべき情報の管理に係る管理責任者を指定し、契約締結後速やかに発注者に通知するものとする。

3 受注者は、保護すべき情報に接する者（受注者及び再委託者等における、派遣社員、契約社員、パート、アルバイト等を含む。以下「取扱者」という。）から情報セキュリティの確保に関する誓約書を徴取するとともに、取扱者の名簿を作成し、同名簿を契約締結後速やかに発注者に通知しなければならない。

4 受注者は、契約締結後速やかに、情報セキュリティ確保のため、取扱者に対し作業内容に応じた教育計画を作成し、発注者の承認を得るものとする。

なお、受注者があらかじめ当該計画を有する場合には、これに代えることができる。

5 発注者は、受注者に対し、第4項の教育計画の実施状況について、報告を求めることができる。

6 受注者は、受注者及び再委託者の資本関係、役員等の情報、本件業務の実施場所、取扱者の所属、専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）、実績及び国籍に関する情報を発注者に通知し承認を得るものとする。

7 受注者及び取扱者は、発注者から本人確認を行うため身分証明書等の提示を求められた場合は、これに応じなければならない。

8 受注者は、情報システム及び機器等や役務の調達におけるサプライチェーンにおける発注者の意図しない変更や機密情報の窃取等が行われなことを保証するための具体的な管理体制を証明する書類を発注者に提出しなければならない。また、第三者機関等による品質保証体制（ISO/JIS Q9001等）、情報セキュリティに関する認証（ISO/JIS Q27001（ISMS）等）取得を証明する書類、情報セキュリティ監査報告書（SOC 2及び3等）等が提出可能な場合は、発注者に提出するものとする。

9 受注者は、情報システム及び機器等・役務の調達におけるサプライチェーンにおける発注者の意図しない変更や機密情報の窃取等が行われるなどの不正が見つかったときに、発注者と連携して追跡調査や立ち入り検査等により原因を調査し、必要な措置を講じなければならない。

（守秘義務）

第4条 受注者は、保護すべき情報を本契約の履行期間中のほか、履行後においても第三者に開示又は漏えいしてはならない。

2 取扱者は、在職中及び離職後においても、保護すべき情報を第三者に開示又は漏えいしてはならない。

- 3 受注者又は再委託者等がやむを得ず保護すべき情報を第三者に開示しようとする場合には、受注者はあらかじめ、書面により発注者に申請し許可を得なければならない。

(管理)

第5条 受注者は、本契約に基づき、保護すべき情報及び及び発注者が受注者に貸与する仕様書その他の資料（以下「業務資料」という。）については、特に厳重な取扱いを行うものとし、その保管管理について一切の責任を負うものとする。

- 2 受注者は、発注者の指定する場所において個別の業務を行う場合に持ち込む物品、保護すべき情報及び業務資料を適正に管理するものとする。また、発注者の承諾なくしては、その場所から物品、保護すべき情報又は業務資料を持ち出してはならない。
- 3 受注者は、前2項の保護すべき情報及び業務資料の管理について、最新の「政府機関等のサイバーセキュリティ対策のための統一基準群」における情報セキュリティ対策に準じた管理を行っていることについて、発注者の承認を得るものとする。
- 4 受注者は、保護すべき情報及び業務資料について、本契約の履行又は発注者の指定した目的以外に使用してはならない。
- 5 受注者は、保護すべき情報について、本契約が終了したとき、又は発注者から廃棄を求められたときは、これを直ちに発注者が認める方法により廃棄するものとする。
- 6 受注者は、保護すべき情報及び業務資料を、発注者の承諾なくしては、方法の如何にかかわらず複製・複写してはならない。
- 7 受注者は、業務資料について、本契約が終了したとき、又は発注者から返還を求められたときは、これを直ちに発注者に返還するものとする。
- 8 受注者は、受注者が作成（複製及び写真撮影を含む。）した文書、図面、図書等（電磁的記録を含む。）又は物件のうち、受注者から発注者に所有権が移転したものは全て発注者の認める方法により廃棄しなければならない。
- 9 受注者は、別途定めがある場合を除き、発注者が特に高い可用性又は完全性の確保が必要と指定する保護すべき情報を取り扱う場合、可用性、通信の速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を発注者と協議し合意文書を作成するとともに、その合意内容について保証しなければならない。

(作業員名簿の通知又は作業責任者の選任)

第6条 発注者は、必要に応じて受注者に当該個別の業務の実施に関する作業を行う者（以下「作業員」という。）の名簿を作業責任者を明らかにした上で作成させ、書面をもって発注者に通知させることができる。ただし、作業責任者は、作業員の中から選任するものとする。

- 2 前項ただし書により選任された作業責任者は、受注者の個別の業務の実施を統括し、受注者の定める規則に基づき就業管理を行い、個別の業務の遂行に関する一切

の事項を処理し、個別の業務の遂行につき受注者を代理する権限を有するものとする。

- 3 受注者が作業責任者の権限に関し制限を設けた場合、作業責任者を変更する場合その他の発注者に通知した内容を変更する場合は、受注者は当該内容を書面により事前に発注者に通知するものとする。
- 4 発注者は、作業責任者又は作業員の個別の業務の遂行について著しく不適當であると認めた場合は、受注者に対して是正のために必要な措置を執ることを求めることができるものとする。

(脆弱性対策等の実施)

第7条 受注者は、本件業務を実施するに当たり、情報システムを使用する場合、当該情報システムのアクセス権の付与を業務上必要な者に限るとともに、保護すべき情報へのアクセスを記録する措置を講ずるものとする。

- 2 前項の場合に、受注者は、情報システムに対する不正アクセス、不正プログラム感染及び情報システムの脆弱性に係る情報を収集し、これに対処するための必要な措置を講ずるものとする。

(調達する機器等や役務における対策の実施)

第8条 受注者は、本件業務を履行するに当たり、調達する機器等や役務がある場合について、あらかじめ発注者にそのリストを提出すること。

- 2 受注者は、前項のリストの提出後、調達する機器等や役務に変更があった場合は、リストを修正し再提出すること。
- 3 受注者は、発注者が調達する機器等や役務について情報セキュリティ上のリスクに係る懸念が払拭できないと判断した場合は、発注者と迅速かつ密接に連携し、代替品選定等を行わなければならない。
- 4 受注者は、本件業務を履行するに当たり、調達する機器等や役務がある場合について、不正な変更（製造工程、流通過程で不正プログラムを含む予期しない又は好ましくない特性を組み込むことをいう。）が疑われると発注者が判断した場合は、受注者において調査及び必要な措置を講じなければならない。

(情報セキュリティの対策の履行状況の確認)

第9条 受注者は、契約締結後速やかに、本特約条項が定める項目を含む情報セキュリティ対策の履行状況（以下「情報セキュリティ対策履行状況」という。）を確認するとともに、確認結果について発注者に報告するものとする。

- 2 受注者は、契約締結後、少なくとも1年に1回、情報セキュリティ対策履行状況を確認するとともに、確認結果について発注者に報告するものとする。
- 3 前各項の確認については、別記様式「情報セキュリティ対策履行状況確認書」によるものとする。ただし、別記様式の様式により難しい場合は、この限りではない。
- 4 受注者は、再委託者等における情報セキュリティ対策履行状況について、前各項に準じた確認の結果を発注者に対して報告するものとする。
- 5 受注者は、発注者に報告した確認結果について、発注者の承認を得るものとする。

6 発注者は、その確認結果が十分でないと認められる場合は、その是正のために必要な措置を講ずるよう受注者に求めることができる。

7 受注者は、前項の規定により、発注者から求めがあったときは、速やかにその是正のために必要な措置を講じなければならない。

(情報セキュリティ侵害事案等事故)

第10条 情報セキュリティ侵害事案等事故（以下「事故」という。）とは次の各号のことをいう。

一 保護すべき情報のほか、契約に係る情報について、外部への漏えい又は目的外利用が行われた場合

二 保護すべき情報のほか、契約に係る情報について、認められていないアクセスが行われた場合

三 保護すべき情報を取り扱う又は取り扱ったことのある電子計算機若しくは外部記録媒体に不正プログラムの感染が認められた場合

四 第5条第9項における合意内容を損なう事故が発生した場合

五 前各号に掲げるもののほか、発注者又は受注者の保護すべき情報のほか契約に係る情報の侵害、改ざん、滅失、紛失、破壊その他の機密性、完全性及び可用性を損なう事故が発生し、又はそれらの疑い若しくはおそれがある場合

(情報セキュリティ侵害事案等事故に関する受注者の責任)

第11条 受注者は、受注者及び再委託者等の従業員の故意又は過失により前条に規定する事故があったときでも、契約上の責任を免れることはできない。

(情報セキュリティ侵害事案等事故発生時の措置)

第12条 受注者は、本契約の履行に際し、第10条に規定する事故があったときは、適切な措置を講ずるとともに、速やかにその詳細を発注者に報告しなければならない。

2 発注者は、第10条に規定する事故が発生した場合、必要に応じ受注者に対し調査を実施することとし、受注者は発注者が行う当該調査について、全面的に協力しなければならない。

3 第10条に規定する事故が再委託者等において発生した場合、受注者は発注者が当該再委託者等に対して前項の調査を実施できるよう、必要な協力を行うものとする。

4 受注者は、第10条に規定する事故の損害、影響等の程度を把握するため、必要な業務資料等を契約終了時まで保存し、発注者の求めに応じて発注者に提出するものとする。

5 第10条に規定する事故が受注者の責めに帰すべき事由による場合、当該措置に必要な経費については受注者の負担とする。

6 前項の規定は、発注者の損害賠償請求権を制限するものではない。

7 受注者は、事故の拡大防止及び再発の防止に関する措置について、発注者に報告しなければならない。

8 受注者は、前項の措置の実施状況について、発注者の求めに応じて発注者に報告するものとし、発注者は、その実施状況が十分でないと認められる場合は、その是

正のために必要な措置を講ずるよう受注者に求めることができる。

- 9 受注者は、前項の規定により、発注者から求めがあったときは、速やかにその是正のために必要な措置を講じなければならない。

(情報セキュリティ監査)

第13条 発注者は必要に応じ、受注者に対して情報セキュリティ対策に関する監査を行うものとし、監査の実施のために、発注者の指名する職員を受注者の事業所その他関係先に派遣することができる。

- 2 受注者は、発注者が情報セキュリティ対策に関する監査を実施する場合、発注者の求めに応じ、必要な協力（発注者の指名する職員による受注者の事業所その他の関係先への立ち入り、関係者への面会、関係書類の閲覧、監査証拠の提出等）をしなければならない。
- 3 発注者が再委託者等に対して情報セキュリティ対策に関する監査を行うことを求める場合、受注者は当該監査の実施のために必要な協力を行うこととする。
- 4 受注者は、自ら内部監査、外部監査及び情報セキュリティ対策に関する監査を行った場合は、その結果を発注者に報告することとする。
- 5 発注者は、監査の結果、情報セキュリティ対策が十分満たされていないと認められる場合は、その是正のための必要な措置を講ずるよう受注者に求めることができる。
- 6 受注者は、前項の規定により、発注者から求めがあったときは、速やかにその是正のための必要な措置を講じなければならない。

(契約の解除)

第14条 発注者は、第10条に規定する事故その他の本特約条項に定める情報セキュリティの確保が困難であると発注者が判断する事実が、受注者の責めに帰すべき事由により発生した場合において、本契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。

- 2 前項の場合において、主たる契約条項の契約の解除に関する規定を準用する。
- 3 発注者は、第10条に規定する事故その他の本特約条項に定める情報セキュリティの確保が困難であると発注者が判断する事実が、受注者又は再委託者の責めに帰すべき事由により発生した場合は、第2条第1項ただし書による承認を取り消すことができる。この場合において、受注者に損害が生じた場合であっても、発注者は一切の責を負わない。

情報セキュリティ対策履行状況確認書

1 確認対象者

- (1) 事業者名：
 (2) 対象部門等名：
 (3) 契約開始年月日：
 (4) 前回確認実施年月日：

【留意事項】

確認対象者が再委託者等の場合は、(1) 欄に事業者名を記載し、その末尾に「(再委託者等)」と記載すること。
 この場合、(3) 欄には、再委託契約等の開始年月日を記載すること。

2 確認事項

番号	確認事項	実施/未実施	実施状況(詳細)又は未実施の理由
1	2. 1 本契約の全部又は一部を第三者に再委託させていない。		
2	2. 1 (1が未実施の場合) やむを得ず再委託をさせるときは、あらかじめ再委託者の商号又は名称及び住所、再委託する業務の範囲、再委託の必要性、再委託期間、再委託率その他の情報セキュリティの確保に係る契約内容等を記した書面を添え、発注者の承認を得ている。		
3	3. 1 情報セキュリティを確保するための体制において事故に関する問合せ窓口を発注者に通知している。		問合せ窓口の連絡先：
4	3. 2 代表者又は代表者から代理権限を与えられた者を情報セキュリティ責任者としている。		情報セキュリティ責任者名：
5	3. 2 情報セキュリティ責任者の下に、保護すべき情報の管理に係る管理責任者を指定し、発注者に通知している。		管理責任者名：
6	3. 3 取扱者から情報セキュリティの確保に関する誓約書を徴収している。		
7	3. 3 取扱者の名簿を作成し、発注者に通知している。		
8	3. 4 教育計画を作成し、発注者の承認を得ている。		
9	3. 6 受注者及び再委託者の資本関係、役員等の情報、本件業務の実施場所、取扱者の所属、専門性(情報セキュリティに係る資格(情報処理安全確保支援士等)・研修実績等)、実績及び国籍に関する情報を発注者に通知し承認を得ている。		
10	3. 7 発注者から身分証明書等の提示を求められた場合は応じている。	※	※
11	3. 8 管理体制を証明する書類を提出している。		
12	3. 8 第三者機関等による品質保証体制、情報セキュリティに関する認証取得を証明する書類、情報セキュリティ監査報告書等を発注者に通知している。	※	※ <input type="checkbox"/> ISO/JIS Q27001 (ISMS) <input type="checkbox"/> ISO/JIS Q9001 <input type="checkbox"/> 情報セキュリティ監査報告書 (SOC2/3 等)

13	3.1 その他、情報セキュリティを確保するために必要な体制を整備している。	※	※
14	4.1 保護すべき情報を第三者に開示又は漏えいしていないことを確認している。		
15	4.2 取扱者が、在職中又は離職後においても、保護すべき情報を第三者に開示又は漏えいしないよう、措置を講じている。		
16	4.3 (1及び2が未実施の場合) やむを得ず保護すべき情報を第三者に開示しようとする場合には、あらかじめ、書面により発注者に申請し許可を得ている。	※	※
17	5.1 保護すべき情報及び業務資料について、特に厳重な取扱いを行っている。		
18	5.2 (発注者の指定する場所において個別の業務を行う場合) 持ち込む物品、保護すべき情報及び業務資料を適正に管理している。	※	※
19	5.2 (発注者の指定する場所において個別の業務を行う場合) 発注者の承諾なくして、その場所から物品、保護すべき情報及び業務資料を持ち出していないか確認している。	※	※
20	5.3 保護すべき情報及び業務資料の管理について、発注者の承認を得ている。		
21	5.4 保護すべき情報及び業務資料について、発注者の指定した目的以外に使用しないよう、措置を講じている。		
22	5.5 保護すべき情報について、発注者から廃棄を求められたとき、直ちに発注者が認める方法により廃棄している。	※	※
23	5.6 保護すべき情報及び業務資料を、発注者の承諾なくして、複製・複写していないか確認している。		
24	5.7 発注者から返還を求められた資料を、発注者に直ちに返還している。	※	※
25	5.9 発注者が特に高い可用性及び完全性の確保が必要と指定する保護すべき情報について、合意文書を作成し、合意内容について保証している。	※	※
26	6.1 (発注者の指定する場所において個別業務を行う場合) 個別業務を行う作業員の名簿及び作業責任者を発注者から求められた場合は通知している。	※	※
27	7.1 (情報システムを使用する場合) 当該情報システムのアクセス権の付与を業務上必要な者に限るとともに、保護すべき情報へのアクセスを記録する措置を講じている。	※	※

28	7. 2 (情報システムを使用する場合) 情報システムに対する不正アクセス、不正プログラム感染及び情報システムの脆弱性に係る情報を収集している。	※	※
29	7. 2 (情報システムを使用する場合) 情報システムに対する不正アクセス、不正プログラム感染及び情報システムの脆弱性に対処するための必要な措置を講じている。	※	※
30	8. 1 (調達における機器等や役務における対策) 調達する機器等や役務がある場合について、あらかじめ発注者にリストを提出している。	※	
31	9. 2 (情報セキュリティ対策の履行状況の確認が2回目以降の場合) 前回の確認及び発注者に対する報告から、1年以上を経過していない。	※	※
32	9. 5 報告した確認結果について、発注者の承認を得ている。		
33	13. 1 (情報セキュリティ侵害事案等事故が発生した場合) 事故発生時に適切な措置を講じるとともに、速やかに発注者に報告を行った。	※	※
34	13. 2 (情報セキュリティ侵害事案等事故が発生した場合) 事故の損害・影響等の程度を把握するため、必要な資料を保存している。	※	※
35	13. 4 自ら内部監査、外部監査及び情報セキュリティ対策に関する監査を行った場合、発注者に結果を報告している。	※	※
確認年月日：			
確認者（事業者名、所属、役職、氏名）：			

【留意事項】

※欄については、該当がある場合に記載する。

別記様式第1号

委託業務着手報告書

令和 年 月 日

宮城県知事 村井 嘉浩 殿

所在地

法人名

代表者

印

下記のとおり業務を開始します。

委託業務の番号	R 8 (委託) 第 号
委託業務の名称	防犯アプリ運用事業
委託業務の場所	
契約締結年月日	令和 年 月 日
委託期間	令和 年 月 日 ~ 令和 年 月 日
契約金額	金 円 (うち取扱に係る消費税及び地方消費税の額 円)
着手年月日	令和 年 月 日
備考	

別記様式第2号

委託業務完了報告書

令和 年 月 日

宮城県知事 村井 嘉浩 殿

所在地

法人名

代表者

印

下記のとおり業務を開始します。

委託業務の番号	R 8 (委託) 第 号
委託業務の名称	防犯アプリ運用事業
委託業務の場所	
契約締結年月日	令和 年 月 日
委託期間	令和 年 月 日 ~ 令和 年 月 日
契約金額	金 円 (うち取扱に係る消費税及び地方消費税の額 円)
完了年月日	令和 年 月 日
備考	