業 務 委 託 仕 様 書

No.	業　　務　　名	業 務 内 容	数 量		単　　価	金　　額	備　　考
1	令和8年度 富谷市情報セキュリティ対策支援業務						
	1.令和8年度情報セキュリティ対策支援業務実施計画の策定	別添仕様書のとおり	1	式			
	2.情報セキュリティポリシー（基本方針・対策基準）及び実施手順の		1	式			
	3.保有個人情報取扱い規程の見直し		1	式			
	4.標的型攻撃メール対応訓練		1	式			
	5.情報セキュリティ監査の実施		1	式			3所属で実施
	6.業務実施報告及び情報セキュリティ対策強化に係る提案		1	式			
	7.情報セキュリティ対策運用に関するアドバイス支援		1	式			
計						(a)	

特記事項			価格計算書		
	履 行 場 所	富谷市　富谷坂松田　地内		(a)　×　1　＝	(b)
				(b)　×　1.1　＝	円
	その他条件等	＜　履行期間　＞ 始　期　：　契約締結日の翌日 終　期　：　令和 9年 3月 31日		価　　格	円
				内消費税相当額	円

令和８年度 富谷市情報セキュリティ対策支援業務仕様書

1. 業務名

令和８年度 情報セキュリティ対策支援業務

2. 業務目的

本件業務委託は、次に掲げる事項を実現するために行うものとする。

(1) 富谷市（以下「本市」という）が保有する情報資産の安全管理対策の強化に向けた啓蒙・啓発活動を推進する。

(2) 国（個人情報保護委員会含む）が示す方向性及び方針等を基に、情報セキュリティポリシー対策基準（令和７年度改定）及び情報セキュリティ実施手順（令和７年度改定）を精査し、新たな脅威等への対策を含めて本市の情報セキュリティ対策の基準及び手順を明確にする。

(3) 職場における情報資産の安全管理対策について標準化及び高度化を図る。

(4) 各業務及び業務システムの運用・保守を行うにあたり、情報セキュリティポリシー対策基準及び情報セキュリティ実施手順の遵守を徹底することで情報セキュリティインシデント発生リスクの低減につながる態勢を確立する。また、業務システムの情報セキュリティ管理態勢の標準化及び高度化を図る。

(5) 保有個人情報の安全な取扱い及びマイナンバー制度の安全な運用を実施することで市民から信頼・信用を得る。

(6) 情報システム所管課が適正に情報システムの運用並びに調達を行うことができる。

3. 履行期間

契約締結日の翌日から令和９年３月３１日まで

4. 履行場所

富谷市　富谷坂松田　地内

5. 業務実施内容

(1) 令和８年度情報セキュリティ対策支援業務実施計画の策定

本市は今年度、情報セキュリティ対策として以下のマネジメント業務を実施する予定である。前年度の実施結果を踏まえて情報セキュリティ対策を強化し、情報セキュリティ管理態勢を高度化するために、委託業務をどのような流れで、また、それらをどのように関連付けて実施するべきかを提案すると共に、各業務の計画を立案する。

① 情報セキュリティポリシー及び情報セキュリティポリシー実施手順の見直し

② 保有個人情報取扱い規程の見直し
③ 標的型攻撃メール対応訓練
④ 情報資産の分類
⑤ 助言型外部監査
⑥ 業務実施報告及び情報セキュリティ対策強化に係る提案
⑦ 情報セキュリティ対策強化に関するアドバイス支援

(2) 情報セキュリティポリシー対策基準及び情報セキュリティ実施手順の見直し

情報セキュリティポリシー対策基準（令和7年度改定）及び情報セキュリティ実施手順（令和7年度改定）を精査し、「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（令和8年3月版）」等の考え方を反映し、国（個人情報保護委員会を含む）からの要請事項や新たな脅威及び脆弱性等に対応するために見直すべき、あるいは見直すことが望ましい事項を提案すること。そこにはガバメントクラウド上に配置する標準準拠システムの利用及び運用を行うにあたり必要なセキュリティ対策も含めると共に、β’モデルを活用して機密性の高い情報資産をインターネット接続系に配置し、当該情報資産をパブリッククラウドサービス上で運用する上での対策も反映すること。

また、本市の情報セキュリティ対策の運用レベルの向上につながる事項も提案すること。

それらの見直し事項については本市による確認及び承認を得ることとし、そのうえで対策基準及び実施手順の改定を行うこととする。なお、改定に伴い新たに必要となる運用様式がある場合は、それを提供すること（提供時期は本市と協議する）。

見直す内容は、以下のガイドラインや計画、手順書等に定められた事項及び要請等についても参照して検討する必要がある。

・地方公共団体における情報セキュリティ監査に関するガイドライン（令和8年3月版）
・自治体情報セキュリティ対策の見直しについて
・特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）【令和7年6月一部改正】
・国による地方公共団体の情報セキュリティ対策の強化について（会計検査院 令和2年1月）
・情報セキュリティインシデント対応ハンドブック（地方公共団体情報システム機構 令和2年3月版）
・小規模自治体のための CSIRT 構築の手引き（地方公共団体情報システム機構 令和5年3月）
・自治体デジタル・トランスフォーメーション（DX）推進計画【第5.1 版】
・自治体 DX 全体手順書【第5.0版】
・自治体情報システムの標準化・共通化に係る手順書【第4.0版】

(3) 保有個人情報取扱い規程の見直し

令和８年改正個人情報保護法を踏まえ、保有個人情報取扱い規程を情報セキュリティポリシー及び情報セキュリティ実施手順、また、特定個人情報の適正な取扱いに関する規程等と整合並びに連携を図り見直すこと。

規定内容は、以下のガイドラインや指針等に定められた事項及び要請等の反映を検討する必要がある。

・個人情報の保護に関する法律についてのガイドライン（行政機関等編）令和８年４月一部改正
・個人情報の保護に関する法律についてのＱ＆Ａ（行政機関等編）令和８年４月更新
・個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）令和８年４月一部改正
・行政機関の保有する個人情報の適切な管理のための措置に関する指針

(4) 標的型攻撃メール対応訓練の実施

標的型攻撃メールによるセキュリティインシデントの発生を抑制すべく職員の意識及び対応力の向上を図ると共に、標的型攻撃メールにおける添付ファイルの開封率及びメール本文中のURLリンクのクリック率、また、これらの行為の傾向等の分析により課題を把握し、今後の対応策を検討することを目的に、訓練を実施する。

訓練にあたって以下を行うこと。

① 訓練メールの件名及び本文の作成
② 訓練メールの添付ファイルの作成
③ 訓練メールの添付ファイル開封後及びメール本文に貼り付けたURLのリンク先で表示する教育用コンテンツの作成
④ 訓練スケジュール及び上記①～③の内容、送信元・送信先メールアドレス等を記した訓練実施要綱の作成
⑤ 訓練結果の収集及び分析
⑥ 実施報告書の作成

訓練条件は以下とする。

① 訓練メールの送信数は、1回の訓練につき300通程度で、訓練は2回実施する。
② 訓練メールは、受託者が保有する訓練の仕組み（ツール・サービス等を含む）を利用し、訓練メール送信環境の設定（送信元・送信先メールアドレスの設定を含む)、訓練メール送信、送信結果の取得等の作業は受託者が行う。
③ 送信先メールアドレスは本市から提供する。
④ 送信回ごとに添付ファイル型とするか､URLリンク型とするかは本市との協議により決定する。
⑤ 送信元ドメインは特に指定しないが、事前に本市へ通知すること。
⑥ 本市は、訓練メールが自治体情報セキュリティクラウド等により隔離されないための対策について協力する。

なお、事前に本市が指定する特定のメールアドレスに訓練メールを送信し、動作確認テスト（リハーサル）を実施する。また、職員に混乱を発生させることのないように業務を履行できるよう計画すること。

(5) 助言型外部監査の実施

① 特定個人情報又は保有個人情報を取り扱う業務所管課（3 課）に対して、助言型の外部監査を実施する。なお、適用基準は以下とする。

a) 富谷市情報セキュリティポリシー対策基準（令和 7 年度改定）

b) 富谷市情報セキュリティ実施手順（令和 7 年度改定）

c) 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(令和 7 年 3 月版)

d) 地方公共団体における情報セキュリティ監査に関するガイドライン（令和 8 年 3 月版）

e) 特定個人情報の適正な取扱いに関するガイドライン行政機関等・地方公共団体等編）【令和 7 年 6 月一部改正】

f) その他、情報セキュリティ等に関し、有用な法律・基準、国からの通知等であって、本市と協議のうえ採用したもの

② 監査は、以下の手順を踏んで実施することとする。

a) 当該年度の監査テーマを決定（本市と協議のうえ）

b) 監査実施計画（監査の目的、監査項目、監査対象業務（主に個人情報を取り扱う業務)、被監査部門、監査手順、実施スケジュール、実施場所、実施体制及び担当者の氏名、本市との役割分担、成果物等を記載）の策定

c) 予備調査の実施

d) 本調査の実施（業務運用実態について訪問調査を実施）

e) 監査調書による事実確認

f) 監査報告（改善提案の提示を含む）

g) 改善計画の確認

③ 補足事項

a) ①で示した適用基準から、本市の実情に合わせて設定した監査項目ごとに具体的な確認事項となる監査要点を列挙した監査チェックシートを作成し、これを基に業務運用実態の訪問調査を行う。従って、監査チェックシートは調査結果を記入することで、監査項目ごとのリスクコントロール度合いが把握できる監査証拠となる。

b) 監査は予備調査にて監査対象となる業務や当該業務で取り扱う情報資産、また利用している情報システム及び情報セキュリティ運用状況に関する基礎情報等を収集したうえで、訪問調査を行うこととする。

c) 監査報告書には、監査証拠に裏付けられた合理的な根拠に基づく意見、制約又は除外事項、その他当該監査の目的に照らして必要と判断した事項を明瞭に記載すること。改善が必要な事項（指摘事項）を記載する場合は、改善すべき理由となる顕在化もしくは残存しているリスク及び具体的な改善提案を記載すること。

(6) 業務実施報告及び情報セキュリティ対策強化に係る提案

上記(1)～(5)にて実施した内容を令和 8 年度情報セキュリティ対策支援業務実施報告書としてとりまとめる。また、(4)、(5)にて実施した結果から本市の課題を導き出し、当該課題への有効な対策に係る提案等を取りまとめた令和 8 年度の総括資料を作成すること。

当該総括資料は、次年度の情報セキュリティ対策支援業務実施計画策定の基礎とする。

(7) 情報セキュリティ対策強化に関するアドバイス支援

本市が実施に向けて検討する情報セキュリティ強化策について、本市の情報システムの運用状況及び情報資産の安全管理対策を踏まえた上で、専門的見地及びセキュリティ強化の観点から助言及び提案を行う。その際、必要に応じて他の自治体の運用状況を参考情報として提示すること。

また、情報セキュリティに関する技術的な脆弱性情報、自治体等における重大事故事例、脅威及びリスク等に関する情報を提供し、実施が望まれる情報セキュリティ対策（技術的・物理的・人的・組織的）について具体的な実施方法等も含めて適宜助言すること。

更に、「自治体デジタル・トランスフォーメーション（DX）推進計画【第 5.1 版】」に基づき、今後、本市がデジタル化の推進を検討するにあたって、情報システムの強靭性向上を含めてセキュリティ上の留意すべき事項等についても助言並びに提案を行うこととする。

なお、情報セキュリティ対策強化のため実施する施策は「(2) 情報セキュリティポリシー対策基準及び情報セキュリティ実施手順の見直し」と関連するため、互いに整合性を持って提案を行わなければならない。

6. 成果物

本件業務委託における成果物は、以下を想定しているが、その他、必要により作成した資料があれば併せて提出すること。提出期限及び提出方法は、本市と協議のうえ決定する。

(1) 情報セキュリティ対策支援業務実施計画
(2) 情報セキュリティポリシー対策基準の見直し案
(3) 情報セキュリティ実施手順の見直し案
(4) 情報セキュリティ実施手順の運用に伴う各種様式（適宜）
(5) 保有個人情報取扱い規程の見直し案
(6) 標的型攻撃メール対応訓練実施要綱
(7) 標的型攻撃メール対応訓練実施報告書
(8) 情報セキュリティ監査実施計画書
(9) 情報セキュリティ監査調書
(10) 情報セキュリティ監査報告書
(11) 情報セキュリティ対策改善計画書（様式のみ）
(12) 情報セキュリティ対策強化に関する提案（令和 8 年度総括）
(13) 令和 8 年度情報セキュリティ対策支援業務実施報告書

7. 監査人要件・履行体制

(1) 情報セキュリティ外部監査の実施に当たっては，主任監査人及び監査人で構成する監査チーム（2人以上）を編成すること。

(2) 本業務の担当者には、以下のいずれかの資格を有する者を1人以上含むこと。

① システム監査技術者
② 公認システム監査人（CSA）
③ 公認情報システム監査人（CISA）
④ ISMS 主任審査員

⑤ ISMS 審査員
⑥ 公認情報セキュリティ主任監査人
⑦ 公認情報セキュリティ監査人
⑧ 情報処理安全確保支援士

(3) 業務責任者は、地方公共団体における以下のすべての業務の実務実績を有すること。
① 情報セキュリティポリシー及び情報セキュリティ実施手順の策定（又は見直し）支援
② 保有個人情報取扱い規程の策定（又は見直し）支援
③ 職員向け情報セキュリティ研修
④ 特定個人情報の安全管理措置に係る研修
⑤ 標的型攻撃メール対応訓練
⑥ 情報セキュリティ自己点検
⑦ 情報セキュリティ外部監査
⑧ 情報セキュリティに関するコンサルティング（マネジメント及びテクニカル分野）

(4) 本業務の受託者は、過去に監査対象業務に関わる情報システムの企画、開発、運用、保守作業及び機器の提供に直接・間接的に携わっている者ではないこと。

8. 資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は本市が妥当と判断する範囲内で受託者に提供する。なお，受託者は、本市から提供された資料は適切に保管し、特に個人情報及び情報システムのセキュリティ対策、情報資産の安全管理に関連する資料の保管は厳格に行うものとする。また、契約終了後は本業務にあたり収集した一切の資料を速やかに本市に返還し、又は廃棄するものとする。

9. 報告等

受託者は作業スケジュールに十分配慮し、本市と密接に連絡を取り業務の進捗状況を報告するものとする。

10. 契約締結後、提出が必要な書類

以下の書類については，契約締結後速やかに本市へ提出すること。
(1) 守秘義務誓約書（任意様式）
(2) 従事者の資格を証明する書類の写し：1部
(3) 過去に監査対象業務に関わる情報システムの企画、開発、運用、保守作業及び機器の提供に直接・間接的に携わっていない旨の誓約書

11. その他

本業務の実施にあたり、本仕様書に記載のない事項については本市と協議のうえ決定するものとする。

以上

【用語解説】

- 監査項目

  監査テーマ（具体的な監査の主題）を細分化した業務運用実態調査の個々の対象

  例）ウイルス対策ソフトの適切な運用、利用者 ID の管理、アクセス記録等の取得及び保存

- 監査要点

  監査項目から細分化した確認事項

  例）ウイルス対策ソフトの定義ファイル更新方法及び更新頻度

- 監査証拠

  監査報告書に記載する監査意見を立証するために必要な事実

  例）監査調書、閲覧資料、閲覧記録等

- 監査調書

業務運用実態調査において、監査人が作成し、又は