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7年度 富谷市情報セキュリティ対策支援業務					
	1. 令和7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対策基準及び実施手順の見直し		1 式			
	3. 職員向け情報セキュリティ研修		1 式			
	4. (特定)個人情報安全管理措置研修((特定)個人情報保護管理責任者向け)の実施		1 式			
	5. 標的型攻撃メール対応訓練		1 式			
	6. 情報資産の重要性分類		1 式			
	7. 自己点検の実施		1 式			
	8. 情報セキュリティ監査の実施		1 式			2所属，1室で実施
	9. 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			
	10. 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		
	履 行 場 所	富谷市　富谷坂松田　地内
	その他条件等	＜ 履行期間 ＞ 始 期 ： 契約締結日の翌日 終 期 ： 令和 8年 3月 31日

価格計算書		
	(a) × 1 ＝	(b)
	(b) × 1.1 ＝	円
	価　　格	円
	内消費税相当額	円

令和７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７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６年度改定）及び情報セキュリティ実施手順（令和６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８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７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 職員向け情報セキュリティ研修

③ （特定）個人情報安全管理措置研修（(特定）個人情報保護管理責任者向け）の実施
④ 標的型攻撃メール対応訓練
⑤ 公文書の分類
⑥ 自己点検
⑦ 外部監査（三層分離のβ’モデルに対応した助言型監査）
⑧ 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
⑨ 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基本方針（令和３年度改定）及び情報セキュリティポリシー対策基準（令和６年度改定)、情報セキュリティ実施手順（令和６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７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、そのうえで基本方針及び対策基準、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７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４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２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４．０ 版】
・自治体 DX 全体手順書【第４．０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】
・サイバーセキュリティを確保するための方針の策定等に関する総務大臣指針について（令和７年３月）

(3) 職員向け情報セキュリティ研修の実施

研修計画を立案し、以下を目的とした研修教材の作成を行い、集合研修にて講師業務を実施すること。なお、集合研修の実施回数等の詳細については、本市と協議の上、決定する。

また、集合研修に参加できなかった職員向けに講義内容を録画した自己学習用 e-Learning 教材を作成すること。録画に必要な機器及びソフトウェア（サービス）は受託者が用意すること。

① 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規程内容を理解し、これに従った運用ができるようになる。

② 前年度の情報セキュリティ点検及び情報セキュリティ監査の結果を基に、留意及び改善すべき事項が認識できるようになる。

③ 情報セキュリティ対策の強化及び情報セキュリティ管理態勢が高度化される。

④ インシデント発生時に、適切な初動対応ができるようになる。

⑤ 昨今の脅威について認識し、理解することができるようになる。

⑥ 情報セキュリティ上の問題点（リスク）を認識し、改善すべき安全管理策を検討することができるようになる。

⑦ 保有個人情報の適正な取扱いに係るポイントを理解し、実践できるようになる。

(4) （特定）個人情報安全管理措置研修（(特定）個人情報保護管理責任者向け）の実施

（特定）個人情報保護管理責任者を対象とし、以下を目的とした研修の計画を立案すると共に、研修教材の作成を行い、集合研修にて講師業務を実施すること。なお、集合研修の実施回数等の詳細については、本市と協議の上、決定する。

また、集合研修に参加できなかった職員向けに講義内容を録画した自己学習用 e-Learning 教材を作成すること。録画に必要な機器及びソフトウェア（サービス）は受託者が用意する。

① （特定）個人情報の漏えい等を防止するための単純な事務ミスをなくす対策に係る着眼点を把握し、定着につなげる。

② （特定）個人情報等のデータ入力業務の委託先に対して必要な監督ができるようになる。

③ （特定）個人情報の漏えい等事案が発生した場合の対応を理解し、実践できるようになる。

④ 保有個人情報の適正な取扱いに係るポイントを理解し、実践できるようになる。

⑤ 令和７年度の実地調査及び立入検査計画を把握する。

⑥ 令和６年度における監視・監督権限の行使状況の概要を把握する。

(5) 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現状の情報セキュリティ対策の問題点を把握し、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１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。

(6) 公文書の分類

本市が行う見直し後の情報セキュリティ対策基準に定める情報資産の分類基準（自治体機密性・自治体完全性・自治体可用性）に基づく公文書の分類分けを支援すること。この新たな基準による分類分けを行うにあたって当該分類基準について詳細に説明し、各分類に該当する公文書の具体例を示した説明資料を作成すると共に、分類分けを行った結果を記載する一覧表（記入例を含む）を作成すること。

なお、分類分けは担当業務ごとに担当所属が行うこととし、受託者は分類分けを行った一覧表の内容を公文書ごとに確認し、問題や疑義があれば問合せを行い、必要により担当所属へ修正を依頼する（修正理由を提示する。)。また、担当所属から質問等があれば対応を行うこと。

前提：担当所属数は３０～４０程度、公文書数：５０～２００程度／担当所属

(7) 自己点検の実施

職員の情報セキュリティに対する意識と現状の運用実態を把握し、課題を可視化するために、以下の事項を前提に、自己点検を実施すること。

① 情報セキュリティポリシー対策基準（令和６年度改定）及び情報セキュリティ実施手順（令和６年度改定)、昨今の脅威と自治体における重大インシデント等を参考にアンケート形式の自己点検シートを作成する。なお、設問数は１０分以内に回答ができる範囲で設定する。
② 昨年度からの職員による運用実態の変化が把握可能な設問を設定する。
③ 標的型攻撃メール対応訓練にて開封（URL クリック含む）した又は開封（URL クリック含む）しなかった理由を調査する設問を設定する。

④ 回収した自己点検シートを課等の所属ごとに集計を行い、集計結果を報告書としてまとめる。なお、報告書には集計結果のみならず、評価及び助言等のコメントを加え、課題を可視化すること。

(8) 外部監査（三層分離のβ’モデルに対応した助言型監査）の実施

① 業務所管課（２課）及び情報システム並びに情報セキュリティの管理部門（１部門、以下管理部門と言う。）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６年度改定）

b) 富谷市情報セキュリティ実施手順（令和６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５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７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６年５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、また利用す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) 管理部門への監査においては、「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７年３月版)」に示されたβ’モデルを採用する場合に必要な監査項目を監査チェックシートに反映すること。また、その場合、本市のネットワーク環境等に基づく脅威や脆弱性になり得る事象への対策状況に係る監査項目も当該シートに盛り込むこと。なお、インターネット接続系及び LGWAN 接続系のセグメントに導入しているセキュリティツール（サービス）及び機器については、その機能や運用方法を確認し、人的及び技術的な観点から脅威と脆弱性を効果的に低減できているかを評価すること。

d) 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。

(9) 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)～(8)にて実施した内容を令和７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、(5)、(7)、(8) 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７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。

(10) 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４．０ 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) 情報セキュリティ研修計画書
(6) 情報セキュリティ研修の教材
(7) 情報セキュリティ研修の自己学習用 e-Learning 教材
(8) （特定）個人情報安全管理措置研修計画書
(9) （特定）個人情報安全管理措置研修の教材
(10) （特定）個人情報安全管理措置研修の自己学習用 e-Learning 教材
(11) 標的型攻撃メール対応訓練実施要綱
(12) 標的型攻撃メール対応訓練実施報告書
(13) 公文書の分類に係る説明資料

(14) 公文書一覧表（記入例のみ）
(15) 情報セキュリティ自己点検シート
(16) 情報セキュリティ自己点検報告書
(17) 情報セキュリティ監査実施計画書
(18) 情報セキュリティ監査調書
(19) 情報セキュリティ監査報告書
(20) 情報セキュリティ対策改善計画書（様式のみ）
(21) 情報セキュリティ対策強化に関する提案（令和７年度総括）
(22) 令和７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 公認情報システム監査人（CISA）
③ 公認システム監査人（CSA）
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

(3) 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。

【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、又は収集した資料