仕　様　書

第1章　総則

第1　目的

本市では、「地方公共団体情報システムセキュリティポリシーに関するガイドライン」に示されるβ'モデルを採用し、クラウドサービスの利活用を前提とした柔軟で効率的な業務環境の構築を目指している。この方針に基づき、現在利用しているGoogle Workspace Enterprise Standard(Chrome Enterprise Premiumを含む。)等(以下「GWS等」という。)において、ゼロトラストセキュリティを中核とした設定を適用し、セキュリティの抜本的な強化と職員の利便性向上を両立させることを目的とする。

特に、Windowsパソコン(以下「1人1台端末」という。)、職員が個人所有するスマートフォン等(以下「BYOD端末」という。)、及びChromebookを含めたマルチデバイス環境において、場所を問わず、安全に業務を遂行できる環境を実現するため、高度な専門知識を有する事業者に対し、運用設計、設定作業及び継続的な運用支援業務を委託するものである。

第2　業務名

令和8年度Google Workspace等運用支援業務委託

第3　履行期間

契約日から令和9年3月31日まで

第4　履行場所

志摩市　地内

第5　対象範囲

本業務の対象範囲は、次に掲げるとおりとする。

1　Google Workspace Enterprise Standard(Chrome Enterprise Premiumを含む。)

2　rakumo for Google Workspace(Basicパック)

第6　監督職員の選任

発注者は、本業務における監督職員を定め、受注者に通知するものとする。監督職員は、契約図書に定められた事項の範囲内において、指示、承諾、協議、本業務の進捗確認及び履行状況の調査等の職務を行うものとする。

第7　実施体制

1　業務責任者の配置

(1)　受注者は、本業務の実施に当たって、業務全体を総括する業務責任者(以下「責任者」という。)を配置すること。

(2)　責任者は、次に掲げる認定資格をすべて有し、日本語に堪能でなければならない。

ア　Googleが認定するAssociate Google Workspace Administrator(又は旧資格名称Professional Google Workspace Administratorを含む。)

イ　Googleが認定するProfessional ChromeOS Administrator

(3)　責任者は、本業務の履行に関し、管理及び統括を行う。

2　実施体制表の作成

(1)　受注者は、業務遂行における体制を明確にし、責任者を含む作業に従事する者の名簿とその連絡先を明記した実施体制表を、本契約締結時に提出すること。

(2)　原則として体制の変更は認めないが、やむを得ず変更する場合は、事前に発注者の承認を得ること。

第8　打合せ協議

本業務を適正かつ円滑に実施するため、責任者は監督職員と主要な区切りごとの打合せを必要に応じて実施するものとし、受注者はその結果を記録し、相互に確認しなければならない。

第9　業務計画書の作成

1　受注者は、契約締結後14日(休日等を含む。)以内に業務計画書を作成し、提出しなければならない。

2　業務計画書には、次に掲げる事項を基本として記載するものとし、実施方針又はその他の事項には、個人情報の取扱い、安全等の確保及び個人情報や機密情報の漏えい防止対策に関する事項も含めるものとする。

(1)　業務概要

(2)　実施方針

(3)　業務工程

(4)　業務組織計画

(5)　打合せ計画

(6)　成果物の内容、部数

(7)　連絡体制(緊急時を含む。)

(8)　その他

3　受注者は、業務計画書の重要な内容を変更する場合は、理由を明確にした上

で、その都度発注者へ変更業務計画書を提出しなければならない。

第10　業務報告書の作成

本業務の実施結果を整理し、業務報告書として取りまとめを行うものとする。

第11　一括再委託等の禁止

1　受注者は、本業務の全部を一括して第三者に委任し、又は請け負わせてはならない。

2　受注者は、本業務の一部を第三者に委任し、又は請け負わせようとするときは、あらかじめ発注者の承諾を得なければならない。

3　発注者は、受注者に対して、業務の一部を委任し、又は請け負わせた者の商号又は名称その他必要な事項の通知を請求することができる。

第12　守秘義務

受注者は、本業務の実施過程で知り得た情報について、発注者の承諾を得ずに第三者へ公表してはならない。

第13　個人情報の保護

受注者は、本業務を処理するための個人情報の取扱については、別記「個人情報・特定個人情報取扱特記事項」を守らなければならない。

第14　セキュリティポリシー等の遵守

受注者は、志摩市情報セキュリティポリシー及び関係法令を守らなければならない。

第15　データ等の保護管理

1　受注者は、発注者が提供した各種資料、並びに本業務の成果物及び記録媒体の内容をなすデータ(以下「データ等」という。)の保護管理について、次に掲げる事項を遵守するものとする。

(1)　データ等の正確かつ適正な維持管理のための措置を講ずる。

(2)　データ等の漏えい、改ざん、汚損、損傷、滅失及びその他事故を防止するための措置を講ずる。

(3)　データ等の授受及び保管等に当たっては、管理台帳等を設け、年月日、内容、数量及び取扱者等を記録する。

(4)　データ等の保管場所について、安全に格納できるよう必要な措置を講ずる。

(5)　コンピュータ室、データ等保管室及びその他本業務の処理に関連する施設について、入退室管理の措置を講ずるとともに、データ等の管理に関し

安全を確保するために必要な措置を講ずる。

2　受注者は、本業務完成後において、次に掲げるデータ等を返還し、又は処分しなければならない。

(1)　発注者から提供された委託業務に係るデータ等は速やかに返還する。

(2)　発注者に納入又は返還を要する物件及び受注者が保管を要する物件を除き、本業務に係る一切のデータ等を、抹消、焼却及び切断等の方法により、再利用できない状態にして処分する。

第16　目的外利用等の禁止

1　発注者は、データ等を当該所属の所管業務以外の目的で使用するときは、データを所管する責任者の承認を得て、受注者に書面で指示するものとする。

2　受注者は、本業務に係るデータ等を本業務以外の目的で利用し、又は第三者に提供してはならない。ただし、あらかじめ発注者の書面による承認を得たときはこの限りではない。

第17　複写及び複製の禁止

受注者は、発注者の指示によるものを除き、本業務に係るデータ等を複写、又は複製してはならない。

第18　データ等の運搬

発注者及び受注者は、データ等の運搬業務の遂行に当たり、管理保全のために必要な措置を講ずるものとする。

第19　立入検査

発注者は、必要があると認めるときは、受注者が本業務を処理するための事務室、コンピュータ室、データ等保管室等の本業務処理に関連する施設を立入検査することができる。

第20　知的財産権の取扱い

1　本業務遂行の過程で行われた発明、創作等によって生じた特許権、著作権、その他の知的財産権(ノウハウを含む。)については、その発明、創作等が発注者又は受注者のいずれかの単独で行われたときは、当該知的財産権はそれを行った当事者に帰属し、共同で行われたときは、発注者及び受注者に共有(持分は寄与分に応じる)で帰属するものとする。

2　発注者及び受注者は、本業務に関し相手方から提供を受けたプログラム、マニュアルその他資料について、それらに関する知的財産権を尊重し、本業務の目的外に利用しないものとする。

第21　事故等発生時の報告義務

受注者は、本業務の遂行において事故の発生により、履行に支障を生じ、又は生じると認めるときは、速やかに事由を付して発注者に報告し、その対策を協議しなければならない。

第22　疑義

本仕様書及び契約約款に定めのない事項又は疑義が生じた場合は、発注者と受注者が協議して定めるものとする。

第2章　業務内容

第23　本業務の概要と進め方

本業務の概要と進め方は次に掲げるとおりとする。

1　本業務の概要

受注者は、本市が採用するβ'モデルおよび本仕様書に示す要件に基づき、GWS等の各種設定を最適化し、セキュリティと利便性を両立した運用を設計する。また、その後の安定した運用に必要なドキュメントを作成し、発注者への知識移転を行うとともに運用を支援する。

2　管理者アカウントの付与

本業務の遂行に当たり、発注者は受注者に対し、GWS等の一時的な管理者アカウントを付与するものとする。また、受注者は、管理者アカウントを利用するに当たり、次に掲げる事項を遵守するものとする。

(1)　管理者アカウントを厳重に管理するとともに、本業務の目的以外に利用してはならない。

(2)　管理者アカウントを用いた定期的な作業について、月次の管理者アカウント利用計画書を前月末までに監督職員へ提出すること。また、当該月の翌月10日までに、管理コンソールの監査ログ等の客観的な証跡を付した管理者アカウント利用実績報告書を監督職員へ提出し、権限の適正利用(濫用がないこと)を証明しなければならない。

(3)　管理者アカウント利用計画書に含まれない臨時的な作業がやむを得ず必要となった場合、監督職員へ口頭等で連絡するものとし、管理者アカウント利用実績報告書へ漏れなく記載すること。

3　本業務の進め方

本業務は、次に掲げるPhaseに従い進めるものとする。

(1)　Phase1：現状設定の調査及び分析

(2)　Phase2：合意形成

(3)　Phase3：設定設計、実装及び運用設計

(4)　Phase4：運用支援

第24　想定スケジュール

本業務の想定スケジュールは次に掲げるとおりとする。なお、全ての設定作業が完了し、運用を開始する日は、令和8年10月5日を予定している。

	7月	8月	9月	10月	11月	12月	1月	2月	3月
Phase1									
Phase2									
Phase3									
Phase4									

第25　本業務の内容

本業務の業務内容は、次に掲げるとおりとする。

1　現状設定の調査及び分析等

2　設定設計

3　設定作業(実装)

4　運用設計

5　運用支援

第26　現状設定の調査及び分析等

次に掲げるとおり現状設定の調査及び分析を実施し、最終的な設定及び運用の方向性について発注者と合意形成を行う。

1　GWS等の詳細な現状設定に関する調査を実施する。

2　調査結果に基づき、本仕様書で示す要件とのギャップ、セキュリティ上の懸念事項、改善点及び設定変更に当たっての確認事項等を整理し、現状設定分析レポートとして提出する。

3　受注者が提出した現状設定分析レポートに基づき、発注者と打合せを行う。

4　打合せでは、現状の課題を共有し、最終的な設定及び運用の方向性について発注者と合意形成を行う。なお、打合せは、必要に応じて複数回実施する。

第27　設定設計

「第26　現状設定の調査及び分析等」の結果を踏まえつつ、次に掲げる要件に基づき、β'モデルの要求事項を満たす最適な設定設計を提案及び実施し、最終的な設定内容を定義した設定定義書を作成の上、発注者の承認を得る。なお、設定定義書の作成及び提案に当たっては、「地方公共団体情報システムセキュリティポリシーに関するガイドライン(最新版)」の記載項目との適合性及び対応関係を明記

し、設定設計の妥当性が客観的に判断できる形で示すものとする。

1　全体方針

β'モデルに準拠したゼロトラストセキュリティモデルに基づき、庁内外のアクセス場所やデバイスを問わず、全てのアクセス要求を検証する構成とすること。

2　アカウント、グループ及び認証基盤

(1)　多要素認証(MFA)

管理者アカウントは常時必須、一般職員アカウントは庁外からのアクセス時に必須とする。認証方式はスマートフォンのプッシュ通知を基本とし、よりセキュアで便利な代替案(FIDO2準拠セキュリティキー等)を提案すること。

(2)　パスワード運用

最低8文字以上で英字と数字又は記号の組合せを必須とする。また、これに加え、推奨される最新の運用ルールを提案し、協議の上で設定すること。

(3)　アクセス制御及びデータ操作制御

Chrome Enterprise Premiumのコンテキストアウェアアクセス及びデータ損失防止機能(以下「DLP機能」という。)を活用し、デバイスの状態とネットワーク環境に基づいた動的な制御を実装する。なお、実装例は次に掲げるとおりとする。

ア　フルアクセス(制限なし)

管理対象のChromebookからのアクセス及び本市のネットワーク(指定IPアドレス範囲内)から接続された管理対象の1人1台端末は、ブラウザ上でのデータ操作制限を設けないこと。

イ　制限付きアクセス(閲覧のみ、DLP機能適用)

BYOD端末からのアクセス及び本市のネットワーク外(テレワーク環境等)から接続された管理対象の1人1台端末は、情報漏洩防止のため、データのコピー&ペースト、印刷、外部サイトへのアップロード及びダウンロード等を制限(閲覧のみ許可)する制御を行うこと。

ウ　認証及び検知シグナル

デバイスが管理対象であること(証明書やシグナル等)及び接続元IPアドレスを正確に識別し、上記「ア」及び「イ」を自動的に切り替える設計とすること。

(4)　Googleグループの設計(動的及び静的の使分け)

ア　一時的なプロジェクトチームなど、メンバー構成の安定性が求められるものは静的グループ(手動管理)で設計すること。

イ　全職員及び所属別メーリングリストや、GWS等内で完結するアクセス権管理(課長職以上等)には、人事異動に自動で追随する動的グループ(自動

管理)を積極的に活用し、管理コストの削減とセキュリティ向上を図ること。

ウ　上記「ア」及び「イ」のハイブリッドアプローチに基づき、グループ全体の体系を設計し、実装すること。

3　デバイス管理

(1)　1人1台端末

Google Chromeブラウザの一元管理を行い、ネットワーク環境の変化(庁内及び庁外)を検知して、前述「2 (3)　アクセス制御及びデータ操作制御」が即座に適用されるよう構成すること。

(2)　BYOD端末

Androidの仕事用プロファイル及びiOSの管理機能を利用し、業務領域とプライベート領域を分離し、業務領域からのデータ持ち出しを制限するとともに、紛失時は業務アカウントと業務データのみを削除すること。

(3)　Chromebook

不特定職員のリモート用端末として一時的に利用するための最適な設定を行うこと。

4　アプリケーション

(1)　Gmail

実行ファイル形式の添付ファイルをブロックし、本人に通知すること。また、送信先ドメインの制限は設けないこと。

(2)　Googleドライブ

全職員の共有範囲は、志摩市役所ドメインを基本とすること。なお、外部との共有は認めないことを原則とすること。

(3)　外部サービス連携

管理者が許可したサービスのみ利用可能なホワイトリスト方式で制御するとともに、利用申請はフォームで行うプロセスを構築すること。

5　セキュリティ監視・運用

セキュリティアラートの一次対応のための具体的なインシデント対応フローを設計すること。

第28　設定作業(実装)

承認された設定定義書に基づき、管理コンソールへの設定作業(実装)を行う。なお、設定作業は、業務への影響を最小限にとどめるため、発注者と調整の上、適切な日時(夜間・休日等を含む。)に実施する。

第29　運用設計

設定作業(実装)完了後、アカウント管理やインシデント対応等の手順をまとめた運用設計書及び職員向け利用ガイドラインを作成する。

第30　運用支援

設定作業(実装)完了後、受注者は発注者に対し、GWS等の円滑な運用を目的とした支援を実施するものとする。

1　GWS等の設定内容及び操作方法に関する疑義照会への回答
2　運用過程で生じた課題や追加設定の要望に対し、技術的知見に基づいた解決策の提示及び代替案の提案
3　その他発注者が求める運用支援(対応の可否及び範囲は双方協議による)

第3章　成果物

第31　成果物

成果物として、次に掲げるものを納入するものとする。

1	業務報告書	1式
2	現状設定分析レポート	1式
3	GWS等設定定義書	1式
4	GWS等運用設計書	1式
5	職員向け利用ガイドライン	1式
6	その他発注者が必要と認める資料	1式

第32　成果物の納入

1　成果物の納入先は、志摩市政策推進部総合政策課とする。
2　成果物は、電子媒体で納入するものとし、データ形式は、Word、Excel、PowerPoint及びPDFに限る。

第33　成果物の帰属

本契約に基づく成果物の著作権(著作権法第27条及び第28条に規定する権利を含む。)は、成果物の引渡しをもって発注者に譲渡されるものとする。ただし、従前より受注者又はその仕入れ先が著作権を有するものについては、著作権は留保されることとする。

第4章　完成検査及び業務委託料の支払い

第34　完成検査

1　受注者は業務を完了したときは、その旨を発注者に通知しなければならない。

2　発注者又は発注者が検査を行う者として定めた職員は、前項の規定による通知を受けたときは、通知を受けた日から10日以内に受注者の立会いの上、設計図書に定めるところにより、業務の完了を確認するための検査を完了し、当該検査の結果を受注者に通知しなければならない。

第35　業務委託料の支払い

1　受注者は、「第34 2」の検査に合格したときは、業務委託料の支払いを請求することができる。

2　発注者は、「1」の規定による請求があったときは、請求を受けた日から30日以内に業務委託料を支払わなければならない。