内部統制システム再構築事業に係る
情報提供依頼書（RFI）

令和８年８月

四国中央市経営企画部情報政策課

（裏面）

ー目次ー

１　概要

本市の内部統制システムは構築から約６年が経過し、耐用年数の到来による機器の更新時期を迎えている。今回の更新にあたっては、本市が３層分離モデルで構築している基幹ネットワークであるインターネット接続系、LGWAN 接続系、個人番号利用事務系の３系統すべての運用管理に係るシステム、サーバ機器及び周辺機器の更新を実施する。

令和９年度の再構築に際しては、国が推進する Government Solution Service（ガバメントソリューションサービス：GSS）の検討動向を踏まえ、2030 年頃に予定される全国的な GSS 完全移行に向けて、段階的移行が可能な柔軟な構成とすることを重視する。

また、クラウド IaaS（基盤提供型サービス）、SaaS（ソフトウェア提供型サービス）の活用、AI を用いたログ分析・異常検知・行動分析、ゼロトラストに基づく端末管理・アクセス制御、クラウド DR（災害復旧）による事業継続性の強化、運用負荷軽減を目的とした DX を取り入れ、省エネ化や有事の際にも必要最低限の業務を継続できる構成とする。

従来の物理構成にとらわれず、設置場所等を含め全面的な見直しを行い、システムの冗長化及び遠隔地データセンターでの運用も視野に入れ、ネットワーク障害や災害時にも強いシステム構築を目的とする。

（１）業務の目的

内部統制システムの更新にあたり、方向性、スケジュール、方法等の検討及び仕様作成の参考とするため、専門的知見を有する事業者から情報提供を受ける。

（２）基本要件

①システム更新に求めるもの

・インターネット接続系、LGWAN 接続系、個人番号利用事務系を利用する市職員を対象とし、全ユーザーを一元管理するため、資産管理機能を必須とすること。
・各端末のアプリケーション及びサービスの動作状況を容易に確認できること。
・事故発生時に迅速にログ検索・追跡ができること。
・危険行為を検知し、管理者への事前警告及び必要な制御が可能であること。また、エンドユーザーにも視覚的に通知し、不正行為の抑止効果を高められること。
・端末の小型化・可搬性向上に伴う紛失・盗難リスクに対し、データ漏えい防止及びリスク軽減が可能であること。
・制限操作について特定条件（利用者指定等）に柔軟に対応できること。
・管理担当者の人事異動時の引継ぎの業務負担を軽減するため、日本語で操作しやすい管理画面を備えること。
・年間１回以上発生する大規模人事異動に対応し、ユーザー権限管理及び人事異動処理を人為的ミスなく迅速に行えること。
・四国中央市公共ネットワークに接続許可を得ていない不正端末を検知・遮断できること。
・庁舎及び外部データセンター等、物理的に離れた拠点に設置するシステムは原則冗長化し、いずれか一方に障害が生じても業務継続できる構成であること。

・LGWAN 接続系及び個人番号利用事務系は、関係省庁が発信するネットワーク分離情報に準拠した構成であること。
・本市の PC へのシステム適用に当たっては、職員の負担を最小限にとどめ、過大な負担なく必要な端末全台へ効率的に資産を配布し適用することができる方法を提案すること。

②ユーザー管理の再構築

・従来のオンプレミス Active Directory による移動ユーザープロファイルおよびフォルダリダイレクト（マイドキュメント等のファイルサーバへの保存）を廃止し、Microsoft 365 の OneDrive を利用したクラウドベースの個人データ管理への移行を検討すること。また、OneDrive の KFM（Known Folder Move）機能を適用し、「デスクトップ」「ドキュメント」「ピクチャ」等のローカルフォルダを、サイレントモードで OneDrive へ自動同期するよう構成すること。
・現在のファイルサーバ（フォルダリダイレクト先）に保存されているユーザーごとの個人データを、OneDrive へ安全かつ確実に移行する手法（Microsoft Migration Manager の使用など）を提示すること。
・ユーザー管理は Active Directory（アクティブディレクトリ）及び Microsoft Entra ID（旧 Azure Active Directory）との連携を重視すること。
・異なるネットワーク間のデータ受け渡しは、厳密な手法によりデータ漏えい防止及びリスク軽減が可能であること。
・同一 ID による二重ログインを防止し、適正な ID 管理が行えること。
・端末ストレージの暗号化により紛失・盗難時のデータ漏えい防止が可能であること。
・エンドユーザーに視覚的警告を行い、セキュリティリスクへの自覚を促す環境を整えること。
・ログ採取は必須とし、ログ解析及び検索機能を強化すること。
・一般職員の行為については全てログ採取を行うこと。

③ クラウド（IaaS、SaaS）を活用した再構築

・インターネット接続系はオンプレミス前提の現構成を見直し、クラウド活用への移行可能性を検討すること。
・ISMAP（政府情報システムのためのセキュリティ評価制度）登録サービスの利用を検討し、ガバメントクラウドとの親和性及び将来的な接続性を考慮すること。
・オンプレミスに残す機能とクラウド移行が適する機能の切り分けを提示すること。
・クラウド活用時のメリットや課題、移行方式を提示すること。
・令和９年度構築後も、GSS 完全移行に向けて段階的にクラウド化を進められる構成とすること。

④ AI によるログ分析・異常検知・行動分析

・AI（人工知能／機械学習）による検知機能を備えたセキュリティソフトの導入を検討すること。
・SSE（セキュリティサービスエッジ）、SASE（セキュアアクセスサービスエッジ）によるクラウド型セキュリティ統合構成を活用し、インシデント検知から対応の自動化・省力化を図ること。

・内部不正、アカウント侵害、未知の脅威の早期検知に資すること。
・少人数体制でも運用可能な日本語対応及び可視化ダッシュボードを備えること。
・将来的に GSS のセキュリティ監査基盤（ログ統合・行動分析）へ移行しやすい構成とすること。

⑤ゼロトラストを踏まえた端末管理・アクセス制御の高度化
・境界防御からゼロトラストへの移行を見据えた構成を検討すること。
・国の検証動向との整合性を考慮すること。
・ID 管理（Active Directory／Entra ID）を軸とした認証統合、MFA（多要素認証）、条件付きアクセス（Conditional Access）を実現すること。
・端末に対するアクセス制御が可能であること。
・令和９年度構築後も、GSS 完全移行に向けて段階的にゼロトラストを強化できる構成とすること。

⑥ 災害・障害時の事業継続性を強化するクラウド DR 構成
・RPO（目標復旧時点）、RTO（目標復旧時間）、RLO（目標復旧レベル）を明示した DR 構成を提案すること。
・バックアップ＆リストア、パイロットライト、ホットスタンバイ、マルチリージョン等の方式ごとのコスト及び復旧時間の比較を示すこと。
・原則クラウドリージョンを活用し、オンプレミス環境に保存するデータについては遠隔地データセンターの利用や庁舎被災時にも必要最低限の業務を継続できるよう検討すること。なお、クラウドリージョンの活用範囲については、当面コスト面を考慮したボリュームとすること。
・将来的に GSS の DR 標準構成へ移行しやすい設計とすること。

⑦ 運用負荷軽減（自動化・省力化）を目的とした DX 要素
・人事異動処理、アカウント発行／削除、権限付与等の定型作業の自動化を検討すること。
・パッチ配信、構成管理、レポート作成等の運用省力化を図ること。
・担当者の異動時の引継ぎ負担を軽減するため、直感的で日本語対応の管理画面を備えること。
・将来的に GSS の運用自動化基盤へ移行しやすい構成とすること。

⑧ オンプレミス／クラウド混在（ハイブリッド）環境の最適な管理体系
・移行過渡期を含め、オンプレミスとクラウドを一元的に管理できる体系を提示すること。
・資産管理、ログ管理、ID 管理を統合的に可視化・統制できること。
・段階的移行の考え方及び各段階での管理体系を示すこと。
・令和９年度構築後も、GSS 完全移行に向けて段階的にハイブリッド管理を縮小できる構成とすること。

（3）コストに対する考え方

本システムの再構築にあたっては、高度なセキュリティ対策と業務効率化を実現しつつも、厳しい財政状況を鑑み、初期導入費用および運用保守費用のトータルコストの最適化を最重要課題の一つとする。

提案事業者においては、以下の考え方に基づき、投資対効果（ROI）が最大となる提案を行うこと。

① 重複機能の統廃合と既存資産の最適化によるコスト削減

新システムで導入するクラウドサービスやセキュリティ製品（EDR 等）、IT 資産管理ツール等の機能により、既存のファイルサーバ、プロキシサーバ、ログ管理・ウイルス対策ソフト等で不要となるシステムや機器を明確にすること。また、これらを積極的に廃止・統合することで、新たなクラウド利用料等の増加分を既存システムの保守・運用費用の削減で相殺し、全体のコスト増を抑制する提案を行うこと。

② ５年間（システムライフサイクル）の総所有コスト（TCO）の明示

見積においては、初期の機器調達・構築費用だけでなく、導入後５年間のライセンス費用、クラウド利用料、運用保守・監視サービス（MDR 等）を含めた「５年間の総所有コスト（TCO）」を明示すること。また、次年度以降のランニングコストにおいて、為替変動やメーカーのライセンス体系変更による予期せぬ費用増のリスクをいかに軽減するか、見解を示すこと。

③ 利用実態に即したライセンスの最適化

市の端末利用実態（１人１台の専用端末、複数人で利用する共有端末、指定管理者用端末等）を検討し、ユーザー単位とデバイス単位のライセンスを最適に組み合わせるなど、オーバースペック・過剰調達とならない最も経済的なライセンス体系を提案すること。

④ 段階的移行による予算の平準化

令和９年度の再構築時点において、全てのシステムを一度にクラウド・ゼロトラスト環境へ移行することで初期費用や初年度の教育・運用負荷が過大となる場合は、国が推進する GSS（ガバメント ソリューション サービス）完全移行の時期（2030 年頃）を見据え、数年をかけて段階的に移行・拡張していくことで、年度ごとの予算を平準化するロードマップを提案すること。

⑤ 複数プランの提示（※RFI における任意要件）

最新の技術や高度なセキュリティ要件を満たす「理想的な構成（フルスペック案）」に加え、コストパフォーマンスを重視し、本市にとって必要十分な要件に絞り込んだ「代替・推奨構成案（コスト最適化案）」など、費用対効果を比較・検討できる複数の概算見積プランを提示することが望ましい。

（4）今後のスケジュール

現在の予定しているスケジュール目安は、次のとおりとする。

項　目	時　期
第１次 情報収集（ＲＦＩ）	令和８年８月下旬～９月下旬
第２次 情報収集（詳細ヒアリング）	令和８年 10 月上旬
更新時期	令和９年度中（令和 10 年 2 月頃の更新完了を想定）

（5）システム利用機器の概要

現在の主なシステム利用機器については、次のとおりとする。

なお、台数については下記の台数より増加する可能性もあるが、ライセンス等については柔軟に対応でき、追加が可能なシステムであること。

項　目	単位	数量	内　訳（利用システム）
・市全職員がそれぞれ 1 つのドメインに所属している。 ・利用者は、ドメインユーザー（一般ユーザー権限）で端末を使用。	デバイス	1,800 （更新対象）	情報系　約 1300 LGWAN 系　約 50 個人番号利用事務系　約 450
	ユーザー	1,200 （更新対象）	情報系　約 1,200 LGWAN 系　約 1,200 個人番号利用事務系　約 1,200
・指定管理者等が独自のドメイン内に所属している。 ・利用者は、本調達外のドメインにて（一般ユーザー権限）で端末を使用。	約 100 台 （プロキシ/URL フィルタリング）		

（６）調達範囲

現時点で想定するシステムの調達範囲は次のとおりとする。

項番	項　目	内　容
1	ウイルス対策 （EDR）	情報系：Aurora Protect LGWAN 系、個人番号利用事務系： Apex One セキュリティエージェント ※更新するシステムに求めるポイント (1) EPP と EDR の統合と軽量動作 既知のマルウェア検知（シグネチャベース）だけでなく、機械学習・AI を活用した未知の脅威を防御する機能（EPP）と、侵入後の脅威を検知・対応する機能（EDR）を、単一の軽量なエージェントで提供できること。エージェントは PC の CPU やメモリ等への負荷が極めて低く、職員の通常業務に支障をきたさないアーキテクチャであること。 (2) 攻撃の全体像の自動紐付けと視覚化 単なるアラートの羅列ではなく、攻撃の根本原因（、影響範囲、タイムラインなどの一連の攻撃プロセスをシステムが自動的に紐付け、一つのストーリーとしてグラフィカルに可視化できること。管理者が直感的にインシデントの全体像を把握でき、ワンクリックで端末のネットワーク隔離やプロセスの停止等の一次対応が行えること。 (3) ランサムウェアおよびファイルレスマルウェア対策 ランサムウェア特有の「大量ファイルの暗号化」といった振る舞いをリアルタイムに検知し、暗号化が進行する前に自動でプロセスを停止・隔離する機能を有すること。PowerShell 等の正規ツールを悪用したファイルレスマルウェアや、メモリ上でのみ実行される高度な攻撃を検知・ブロックできること。 (4) 専門家による 24 時間 365 日の監視・対応支援（MDR サービス）の必須化 市の運用負荷を軽減するため、メーカーまたは専門のセキュリティアナリストによる 24 時間 365 日の監視・分析・対応支援サービス（MDR：Managed Detection and Response）が標準またはオプションで提供されること。日本語による対応および国内拠点からのサポートが提供されること。 深刻なインシデントが発生した際、アナリストからの電話やメールによる即時通知、および推奨される具体的な対応手順の提示が行われること。
2	グループウェア	情報系：株式会社ネオジャパン desknet's NEO ※更新するシステムに求めるポイント 運用コストを低減しつつ、エンドユーザーが使いやすい直感的な GUI を備えていること。

3	IT 資産管理ツール	MOTEX 株式会社 Lanscope エンドポイントマネージャーオンプレミス版 ※更新するシステムに求めるポイント (1) 運用負荷を軽減する直感的な操作性 専任の IT 管理者が不在、または人事異動による担当者変更時であっても、直感的に操作が可能な日本語対応の GUI を備えていること。クライアント PC の稼働状況やアラート状況が、アイコン等で視覚的に一覧できるダッシュボード機能を有すること。 (2) 内部不正を抑止する視覚的な警告（アラート）機能 セキュリティポリシーに違反する操作（許可されていない USB 接続、特定サイトの閲覧、業務外アプリの起動等）が行われた際、エンドユーザーの PC 画面上に警告メッセージ（ポップアップ等）を視覚的に表示し、不正操作の抑止や注意喚起ができること。警告メッセージの内容は、市が任意の文章にカスタマイズできること。 (3) 柔軟で詳細なデバイス（USB 等）制御 USB メモリ等の外部記憶媒体の利用について、一律の禁止・許可だけでなく、個体識別（シリアルナンバー等）による特定デバイスのみの許可設定ができること。一時的な業務利用を想定し、「読み取り専用」での許可や、「特定期間・時間帯のみの利用許可」など、柔軟な権限設定が行えること。 (4) 遠隔地拠点を支援するリモート操作機能 出張所や市内公共施設に設置された端末のトラブル解決を支援するため、管理画面から対象 PC へのリモートデスクトップ（画面共有・遠隔操作）が追加ライセンスなしで行えること。 (5) 他社セキュリティ製品連携によるインシデント時の自動遮断 導入予定のウイルス対策ソフト（エンドポイントセキュリティ）や UTM 等のネットワーク機器と連携できること。マルウェア感染や危険な通信を検知した際、管理者の手動操作を待たず、該当端末を自動的にネットワークから遮断・隔離する機能を有すること。
4	暗号化ツール	Microsoft 社　Bitlocker で構築 ※更新するシステムに求めるポイント 従来の「ディスクドライブ単位の暗号化（OS 標準機能の Bitlocker）」による端末紛失対策に加え、ゼロトラストの観点から「データ（ファイル）そのもの」を保護し、二次漏洩を防ぐため、以下の要件を満たすシステム（IRM/DRM）を提案すること。 (1) ファイル単位の自動暗号化と透過的な操作性 ユーザーによる手動のパスワード設定や暗号化操作を必要とせず、ファイルの作成・保存時にシステムが自動的にファイル単位で暗号化を行うこと。

4	暗号化ツール	正規の権限を持つユーザーがファイルを開く際は、パスワード入力等の手間なく、通常通りアプリケーションが起動する「透過的な操作性」を備え、業務効率を低下させないこと。 (2) 外部持ち出し・流出後の二次漏洩防止 ファイルが端末から USB メモリへのコピー、メールへの添付、またはクラウドストレージ等へ移動・持ち出された場合でもファイル自身の暗号化状態が維持されること。万が一、ファイルが外部へ流出（誤送信や持ち出し）した場合であっても、市の Active Directory 等の認証基盤で許可されていない第三者はファイルを閲覧・解読できない仕組みであること。 (3) 多様なファイル形式への対応 Microsoft Office ファイル（Word, Excel, PowerPoint 等）だけでなく、PDF、テキストファイル、画像ファイル、CAD データ、一太郎など、業務で利用する多様な拡張子・アプリケーションのファイルを暗号化対象として扱えること。 (4) 細やかなアクセス権限制御と操作制限 暗号化されたファイルに対し、ユーザーやグループ単位で「フルコントロール」「編集可能」「閲覧のみ」といったアクセス権限を付与できること。必要に応じて、権限のないユーザーによる「印刷の禁止」「テキストのコピー＆ペースト禁止」「画面キャプチャ（スクリーンショット）の禁止」などの操作制御が行えること。 (5) 既存のファイルサーバおよびクラウドストレージへの適用 移行過渡期における既存のオンプレミスファイルサーバや、将来的なクラウドストレージ（OneDrive や SharePoint 等）上のファイルに対しても、一括での暗号化や権限付与が可能であること。
5	ディレクトリ・サービス	Active Directory(Windows Server 2019)で構築
6	プロキシ/URL フィルタリング	四国中央市ネットワークに接続する端末が利用。
7	ファイルサーバ	ファイルサーバを設置し、各端末のマイドキュメントをリダイレクトして使用。 ※クラウドリージョンの活用を検討すること
8	プリントサーバ	情報系：約 150 種類のプリンタを登録して使用。 個人番号利用事務系：約 50 種類のプリンタを登録して使用。
9	WSUS サーバ	四国中央市ネットワークに接続する端末が利用。
10	LGWAN 振り分けシステム	四国中央市職員が利用している。
11	二要素認証システム	個人番号利用事務系： 日本電気株式会社　NeoFace Monitor パッケージ版

（7）システム利用情報

現在の主なシステム利用情報については、次のとおりである。

項番	項　目	内　容
1	端末設置場所	四国中央市本庁及び市内公共施設 （出張所、保育所、幼稚園の市内公共施設等）
2	端末 OS	Microsoft Windows11 Pro
3	メモリ	8.0GB～16 GB
4	利用ブラウザ	Microsoft Edge 等
5	業務 アプリケーション	主なオフィスソフトウェア Microsoft 365 Apps for enterprise ※別途調達でリプレース予定（本件調達の内容を実現するために E3 ライセンスへの移行を予定している）
6	Windows CAL	Windows 2019 CAL を 3,100 ライセンス保有 Windows 2025 CAL を 600 ライセンス保有
7	DHCP	固定 IP を必要としない端末は、概ね DHCP による動的アドレスを使用している。
8	その他 アプリケーション	QommonsAI、Kintone、Adobe Reader 等

２　情報提供依頼事項

情報提供を依頼する内容は、次のとおりとする。

（１）更新の手法に関すること

安全・確実に実施するための手順、手法、支援ツール等の情報提供。

（２）保守内容に関すること

次年度以降の保守内容及び概算見積（任意様式）。

（３）将来における拡張性に関すること

機器の物理的な拡張以外にも運用保守面での拡張性提案。

（４）スケジュールに関すること

今後のスケジュールを基本とし、本稼動までのスケジュールの提供。

（５）見積り費用に関すること

更新に関しての概算見積（任意様式）。

（６）導入実績に関すること

他の自治体の導入実績についての情報提供。

なお、可能な限り機器構成や運用経費等についての情報提供。

（７）障害発生時の対応に関すること

障害時の対応や大規模災害発生時における BCP の観点から対応手法等の提供。

３　情報提供要領

情報提供手順は、次のとおり

（１）申込方法

事前の申込み等は不要です。

（２）提出期限

令和８年９月 30 日（水）午後５時まで

（３）提出方法

四国中央市手のひら市役所 電子申請フォームよりご提出ください。紙資料の提出は不要です。

（申請フォーム URL）

https://apply.e-tumo.jp/city-shikokuchuo-ehime-u/offer/offerList_detail?tempSeq=12588

（４）資料形式

①Ａ４サイズ（縦横自由かつ任意の様式）。

②提案書には、会社名、住所、代表者名、連絡担当者名、連絡担当者の電話番号、FAX 番号、メールアドレス等を記載。

③提供データは Adobe Reader、Microsoft Office 、Microsoft Edge 等の一般的なソフトウェアにより閲覧が可能な形式。

（５）当該案件にかかる質疑

当該案件にかかる質疑は、次項の問合せ先までメールにて行うこと。

（６）問合せ

〒799－0497　愛媛県四国中央市三島宮川４丁目６番 55 号

四国中央市　経営企画部　情報政策課　システム管理係

TEL：0896-28-6204

E-Mail：johoseisaku@city.shikokuchuo.ehime.jp

（７）その他特記事項

①本提案の実施に要する費用は、各提案者の負担とします。

②本提案依頼は、現在各事業者において保有している技術情報や価格等の情報を得るための手段であり、御社からどのようなご提案をいただいても、それをもって将来の契約を約束するものではありません。

③本提案は、内部統制システム再構築事業に係る基礎資料を整備するために情報の提供を依頼するものであり、今後のスケジュールを含め、事業の実施そのものについても保証するものではありません。

④ご提供いただいた情報・資料については返却いたしません。

⑤ご提供いただいた情報・資料に関して、後日問い合わせ等を行う場合があります。

⑥ご提供いただいた情報・資料は、今後の調達仕様の検討その他本ＲＦＩの目的の範囲内で利用します。また、四国中央市情報公開条例に基づく公文書開示請求があった場合は、同条例の定めに従い、公開の対象となることがありますが、公開により事業上の利益を害する恐れがある情報については、不開示情報に該当するかを個別に判断しますので、該当箇所及びその理由を明示してください。なお、本件は契約締結までは、全文を不開示として扱います。