

コミュニケーション・プラットフォーム
構築及びネットワーク更改業務仕様書

令和 7 年 4 月

徳島県企画総務部情報政策課行政DX推進室

内容

1 業務の概要	1
2 業務概要	1
2.1 構築業務	1
2.2 技術支援等	1
3 構築業務にかかるプロジェクトの管理要件	1
3.1 プロジェクトの体制	1
3.2 プロジェクト管理等	1
3.3 プロジェクトの進め方	2
3.4 現行業者との調整	2
4 本業務仕様書についての注意事項	2
5 構築業務にかかる各種提出書類	2
6 環境構築に係る要件	3
6.1 共通要件	3
6.2 セキュリティ全般に関すること	3
6.3 MDM、MAM に関すること	4
6.4 Chrome ブラウザに関すること	4
6.5 アカウントに関すること	5
6.6 メールに関すること	5
6.7 ドライブに関すること	6
6.8 施設等の予約に関すること	6
6.9 年度異動等の処理に関すること	6
6.10 担当者名簿とグループ及びスペースの作成に関すること	6
6.11 ネットワークに関すること	6
7 データ移行に係る要件	7
7.1 メールデータの移行に関すること	7
7.2 ファイルサーバーのデータ移行に関すること	7
7.3 施設等予約のデータ移行に関すること	8

7.4 検証環境テナントのデータ移行に関すること	8
7.5 その他のデータ移行に関すること	8
8 β モデル移行に伴う事前監査への協力について	8
9 GWS、CEP 及び本業務で構築したネットワークの技術支援等	8
10 その他	9

1 業務の概要

本県が導入する、Google Workspace Enterprise Plus（以下、「GWS」という。）及び Chrome Enterprise Premium（以下、「CEP」という。）について、環境構築、技術支援等を行うものである。

2 業務概要

2.1 構築業務

業務対象期間は令和 7 年 6 月 1 日から令和 8 年 3 月 31 日まで。

県による積算上の上限額は、消費税を含み 1 2 6 , 1 9 5 千円である。なお、予定価格は別途定める。

2.2 技術支援等

業務対象期間は令和 7 年 10 月 1 日から令和 12 年 5 月 31 日まで。

県による積算上の上限額は、消費税を含み 6 0 , 3 3 5 千円である（月単位で同額）。なお、予定価格は別途定める。

3 構築業務にかかるプロジェクトの管理要件

3.1 プロジェクトの体制

1. 本業務受託事業者は、令和 7 年 3 月 28 日時点で Google Cloud プレミアパートナー及び Google Workspace プレミアパートナーの両方を Google 社から認定されていること。
2. 本業務受託者は ISO/IEC27001(JIS Q 27001) 認証を取得していること。
3. 本業務を確実に遂行するために、過去に Google Cloud Partner Top Engineer アワードプログラムを受賞している者が少なくとも 1 名含まれた履行体制（支援体制を含む。）を確保していること。
4. 過去 3 年以内に都道府県庁のネットワークの設計及び設定に携わったネットワーク技術者がメンバーとして参加していること。なお、本県に申請の上、本業務への参画を承認された事業者（以下、「協力事業者」という。）の技術者でも可とする。
5. 本業務について十分な知識を有するものが責任ある立場でプロジェクトに当たること。
6. 本業務に従事する者は、本県並びに関係者と十分な協力が図れる体制とすること。

3.2 プロジェクト管理等

1. 本業務受託事業者は契約締結後速やかに本業務仕様書 5 に示す業務計画書を作成の上、本県の

承認を得た上で業務に取りかかること。

2. プロジェクトの遂行に当たり、業務計画書の内容に変更が必要となる場合、本県と協議し、承認を得ること。
3. 必要に応じて適宜打合せ等を実施し、本県に対し報告及び作業内容の説明・協議を行うこと。

3.3 プロジェクトの進め方

1. 本県と本業務受託事業者は、工期内にプロジェクトが完了するよう、双方が誠意をもって対応すること。
2. 本業務受託事業者は契約後速やかに構築作業に着手すること。なお、設計協議を開発作業と平行して行うなど、工期短縮に努めること。
3. 進捗会議は 1 週間に 1 回程度開催すること。

3.4 現行業者との調整

1. 本業務の履行上、本県の全庁 LAN 運用管理受託事業者、プライベートクラウド運用管理受託事業者及び各業務システム担当事業者と調整等が必要となる場合は、本業務受託事業者の責任により調整すること。
2. 当該調整に係る費用を本県に請求することはできない。

4 本業務仕様書についての注意事項

1. 全ての作業、保守、表示、文書で使用する言語は、原則日本語とする。
2. 本業務について、委託契約書及び本業務仕様書に明示されていない事項でも、その履行上当然必要な事項については、本業務受託事業者が責任を持って対応すること。
3. 本業務仕様書に記載されている全ての業務に対し、いかなるケースにおいても本県に対し、別途費用を請求することはできない。ただし、本県の事情による仕様変更で追加費用が発生する場合については別途協議を行うこととする。
4. 本仕様で定めのない事項が発生した場合及び疑義が発生した場合は、本県と協議の上、定めるものとする。

5 構築業務にかかる各種提出書類

1. 受託事業者は「表 1」の書類（以下、「提出書類」という。）を作成すること。
2. 提出書類に関して、事前に本県に対し十分な説明を行い、内容の承認を得ること。
3. 提出書類は、Google のオフィス・アプリケーションで作成すること。

表 1 提出ドキュメント一覧

No.	提出物	提出期限
1	業務計画書（全体工程表及び実施体制図）	契約締結後速やかに提出
2	会議の要点整理書	各会議終了後速やかに提出
3	課題管理表	随時
4	作業進捗報告書	随時
5	各種パラメーターシート	設定終了後速やかに提出

6 環境構築に係る要件

6.1 共通要件

1. 4,760 人が同時に操作して、遅延が発生しない十分な構成とすること。
2. 本システムのサービス提供時間は 24 時間 365 日とする。
3. GWS 及び CEP のライセンス各 4,760 について、利用に必要な設定を行うこと。
4. 本県が指定するドメインで環境を構築すること。なお、プライマリドメインは、pref.tokushima.lg.jp で、これ以外に 6 つのサブドメインが存在することを考慮し、設計及び構築を行うこと。
5. 管理者権限で設定可能な主たる機能について本県に説明、設定案を提示し、了解を得た上で作業を開始すること。なお、セキュリティに関する設定については、すべて本県に説明すること。
6. 本業務に必要なドキュメントは GWS 上に用意すること。
7. Windows、macOS、ChromeOS、iOS、Android のクライアントでの利用を想定すること。
8. Google Cloud のリージョンは国内とすること。
9. ライセンスについて、GWS 及び CEP の構築開始は令和 7 年 8 月 1 日から、職員による GWS 及び CEP の利用開始は同年 10 月 1 日から、Identity-Aware Proxy（以下、「IAP」という。）については、遅くとも令和 8 年 1 月末から、利用が開始できること。

6.2 セキュリティ全般に関すること

1. 庁外からのアクセスについて、情報セキュリティの観点からクライアントのコンテキストに基づいたアクセスレベルの割り当て案を提示し、県に承認の上、設定を行うこと。

2. 業務用 PC とそれ以外を分類し、それぞれにコンテキスト・アウェア・アクセスで設定するポリシー割当ができるよう設定すること
3. 情報資産の漏洩を防ぐ観点から、データ保護ルールを提案し、県に承認の上、設定を行うこと。
4. BYOD やリモートワークを想定したコンテキスト・アウェア・アクセスの設定を、県と協議の上、行うこと。BYOD については、携帯デバイス（iOS / Android）のブラウザ・ネイティブアプリそれぞれに対してアクセスを制御し、更にデータを外部共有できない仕組みを設計、実装すること。
5. 業務用 PC から本県以外の GWS テナントに対しアクセスできない設定を行うこと。
6. 庁内ネットワークから Google 社の各種サービスを利用する際、管理者が許可していないアカウントからのアクセスを制御できること。
7. ユーザーアカウント毎のアクセスやアプリの利用制限だけでなく、端末のアクセス制御、ポリシー配布、DLP（データ損失防止）、分類ラベルを含めた組み合わせによるセキュリティ制御を実装すること。
8. 画面キャプチャを禁止すること。
9. 庁外からのアクセスの場合、印刷をできないようにすること。

6.3 MDM、MAM に関すること

1. Android、iOS、Chromebook に対して、MDM 及び MAM の設定を行うこと。MDM、MAM に必要な連携サービスの設計・設定も含むこと。Google Workspace や CEP だけでなく、Apple Business Manager なども含めた設計・設定ができること。
2. 仕事用プロファイルにおいて、インストールできるアプリを制限すること。
3. 仕事用プロファイルから個人用プロファイルに対してコピー&ペーストができない設定とすること。
4. 仕事用プロファイルから個人用プロファイルに対してデータの持ち出しができない設定とすること。

6.4 Chrome ブラウザに関すること

1. 業務用 PC のブラウザを「管理対象ブラウザ」として登録するために必要な設計・設定を行うこと。
2. シークレット モードを無効とすること。
3. サードパーティのコードを実行できないようにすること。
4. 高度な保護機能プログラムを有効とすること。
5. 安全でないメディアのキャプチャを拒否する設定とすること。
6. サードパーティのコンテキスト内の WebSQL を許可しない設定とすること。

7. 安全でないコンテキストでの WebSQL を無効とすること。
8. 安全でないフォームでの入力に警告を出す設定とすること。
9. 古い Flash の実行を許可しない設定とすること。
10. セーフ ブラウジングによる保護を強化すること。
11. 全てのダウンロードファイルに対して、セーフブラウジングチェックを行うこと。
12. 不正なコンテンツを含むサイトを開くことを許可しない設定とすること。
13. セーフブラウジングにおいてダウンロードの詳細スキャンを有効とすること。
14. ユーザーに Enterprise Connector を有効とすること。
15. リアルタイムでの URL のチェックを有効とすること。
16. 暗号化されたファイルのダウンロードを禁止すること。
17. 新しいプロファイルの追加を無効にすること。
18. ゲストモードでのブラウザへのログインを禁止すること。
19. 上記以外の設定について、案を提示し、県の承認を受け、設定作業を行うこと。

6.5 アカウントに関すること

1. 既存の LDAP Manager と同期できる仕組みを構築し、アカウント・グループ設計を実施した上で、同期対象の制御（LDAP クエリ開発含む）や Google Workspace ライセンス運用を最適化すること。また、同期において LDAP Manager に属性定義が必要な場合は LDAP を理解して正確な情報を提供すること。なお、LDAP Manager の設定等については本業務の対象外とする。
2. 運用上、既存 LDAP Manager で管理されないアカウント・グループが必要な場合は個別管理する仕組みを準備すること。
3. パスワードについて既存 LDAP Manager と同期すること。
4. 各所属ごとにグループを作成し、全てのユーザーについて適切なグループに割り当てること。
5. すべての機能が使える職員と、機能制限付き職員とでグループを分けること。

6.6 メールに関すること

1. インターネットメール及び LGWAN メール振り分けを意識したメール・ルーティングを行うこと（別紙、概念図 1 参照）。
2. アカウントごとに固有のメールアドレスを作成すること。
3. 所属ごとの代表メールアドレスを作成すること。
4. 現環境で任意に作成したメールアドレスを新環境においても作成すること。左記については、複数の異なるドメインがあることに留意すること。
5. 個人情報等を本文や添付ファイルに含んでいる場合は、送信時に警告メッセージを出すこと。
6. 危険性の高いと判断されるメールはドロップする設定とすること。

7. 外部ドメインへの送信に際しては、警告メッセージを発すること。
8. DKIM を有効にすること。
9. POP 及び IMAP アクセスを無効とすること。
10. 受信メールを自動転送させない設定とすること。
11. ユーザーごとの送信ゲートウェイを許可しない設定とすること。
12. 外部宛先への送信に対して警告を表示する設定とすること。
13. 安全性に関する設定についてはすべて有効とすること。詳細な設定が必要な場合は県と協議すること。
14. メール配信前のスキャンを強化する設定とすること。
15. マルウェアとフィッシングに対する保護を強化する設定とすること。
16. セキュリティ サンドボックス機能を有効とすること。

6.7 ドライブに関すること

1. 職員が外部テナントに公開できる共有ドライブを作成させないこととし、必要な場合は承認行為を含む申請および共有ドライブの作成・権限付与を自動で処理できる仕組みを構築すること。また全体的な利用状況の棚卸しが 1 オペレーションで実施できること。
2. 「AI 分類」について、県と協力し「ラベル自動適用」が有効に働くよう助言を行うこと。
3. 現行ファイルサーバーにおいて設定されているアクセス権限を新環境に再現すること。

6.8 施設等の予約に関すること

1. 会議室及び備品リソースを集中管理できる仕組みを提供すること。
2. 初期リリース時に 500 程度の会議室及び備品リソースの登録を実施すること。
3. 施設予約に当たっては、承認処理を前提としたワークフローを用意すること。

6.9 年度異動等の処理に関すること

1. 年度異動や組織改編を想定し、GWS 運用者に負荷がかからない自動化の仕組みを講じること。

6.10 担当者名簿とグループ及びスペースの作成に関すること

1. AppSheet を使い、各業務の担当者の申請を契機として、台帳（スプレッドシート）、各業務別の担当者グループの自動作成ができる仕組みを構築すること。

6.11 ネットワークに関すること

1. 庁内のネットワーク層は、DMZ(以下、「Lv.1 層」という。)、インターネット接続層<サーバー設置領域> (以下、「Lv.2a 層」という。)、インターネット接続層<行政事務用 PC 設置領域> (Lv.2b)、内部ネットワーク層<サーバー設置領域> (以下、「Lv.3 層」とい

う。）、LGWAN 接続層（Lv.4）で構成し、層を跨ぐ通信は原則できない仕組みとしている。このことは、本業務の遂行にあたっての前提条件である。全庁 LAN 内の Web システムへのアクセス経路は、庁内ネットワークの層を前提として Google Cloud においてもネットワーク分離、通信制御を実現すること。

2. 全庁 LAN 内外に位置する行政事務用 PC から GWS が利用できるよう、環境を構築すること（別紙、概念図 2 参照）。
3. 上記 2 及び 3 について CEP の利用を強制する仕組みとすること。
4. 全庁 LAN 内外に位置する行政事務用 PC（Windows）及び BYOD 端末（ChromeOS）について、全庁 LAN 内の Web システムにアクセスできる IAP 環境を構築すること（別紙、概念図 3 参照）。左記 Web システム数は、Lv.2a 層に約 40、Lv.3 層に約 60 とする。なお、IAP の運用は本業務の対象外とする。
5. IAP は、Cloud Identity と連携すること。
6. 上記 4 のため Google Cloud と庁内ネットワークとのアクセス回線として、200Mbps の閉域回線（Partner Interconnect）を 2 本、本県が用意するものとする。
7. 庁内から GWS への接続及びインターネットへの接続用として、1 Gbps ベストエフォート且つ 100 Mbps 帯域確保相当のインターネット回線を 2 本、本県が用意するものとする。
8. 県が現在運用している機器等に必要な設定変更は、本業務の対象外とする。

7 データ移行に係る要件

7.1 メールデータの移行に関すること

1. メールデータは移行しないものとする。

7.2 ファイルサーバーのデータ移行に関すること

1. 移行条件は次のとおりとする。
 - 移行対象データ量 140TB 程度
 - 接続プロトコル：SMB
 - 移行用回線 1 Gbps（ベストエフォート）2 本（本県が調達）
 - 現行のフォルダ構成：「所属 - 年度（5 年分）」
 - 所属フォルダ数は、約 300 である。
 - 現行は、所属フォルダに対して当該所属の全職員に閲覧、編集権限が付与され、配下のフォルダに権限が委譲されている。
 - 現行は、所属ごとに特定の職員だけに権限が任意に付与できるフォルダが複数ある。
2. ファイルサーバは常に更新されているため、利用開始において最新化の処理を講ずるなど含めた移行計画を立案し移行環境含めた設計・構築をすること。

3. 移行できないデータについては県と協議の上、本県の指示に従うこと。
4. 一部所属においては、令和 7 年 10 月 1 日に運用を開始でき、遅くとも令和 7 年 12 月 26 日までには、各所属の「令和 7 年度フォルダ」は全て、その他のフォルダは令和 8 年 3 月中旬には移行が完了していること。

7.3 施設等予約のデータ移行に関すること

1. 現行の予約データは移行しないものとする。
2. 令和 7 年 10 月 1 日から運用を開始できること。

7.4 検証環境テナントのデータ移行に関すること

1. 「gws.pref.tokushima.lg.cloudg.jp」のテナントから、メール、カレンダー、ドライブのデータを移行すること。
2. 令和 7 年 10 月 1 日までに、移行を終えること。

7.5 その他のデータ移行に関すること

1. 現行のデータは移行しないものとする。
2. 職員自らがデータ移行できるよう、マニュアルを作成すること。

8 β モデル移行に伴う事前監査への協力について

1. 本業務受託者は、本県が β モデル採用のため受ける監査について、本業務範囲に関し責任を持って対応すること。
2. 上記 1 の監査は、総務省「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 5 年 3 月版）」（以下、「監査ガイドライン」という。）における組織的・人的対策に係る監査項目（23 項目）及び「3.12. β モデルを採用する場合の追加監査項目」（10 項目）が対象である。

9 GWS、CEP 及び本業務で構築したネットワークの技術支援等

1. 運用事業者は県が別に指定する（本業務の対象外）。
2. 運用事業者で解決できない問題が発生した際の技術支援を行うこと。技術支援の対象は、調達済みライセンスサービス（GWS / CEP）だけでなく、本調達の構成要素となる Google Cloud や Apple Business Manager、利用端末 OS（Windows、macOS、ChromeOS、iOS、Android）とすること。
3. 障害発生時や偶発的な要件追加時の、技術検証と結果報告をすること。技術検証や報告の対象は調達済みライセンスサービス（GWS / CEP）だけでなく、本調達の構成要素となる

Google Cloud や Apple Business Manager、利用端末 OS（ Windows、macOS、ChromeOS、 iOS、Android ） とすること。

4. 運用事業者向けガイド及びトレーニングを提供すること。左記トレーニングは録画の配信を可能とすること。
5. 導入時、一般職員向け GWS の概要や注意点などについて、1 回以上 Google Meet 上で説明会を開催し、その録画の配信を可能とすること。
6. 一般職員向けトレーニングを年 1 回以上実施すること。
7. 運用事業者向けトレーニングを年 1 回以上実施すること。

10 その他

1. 本業務により構築した Google Cloud に係る各サービスの利用料（役務費）については、本業務には含まないものとする。