別紙２

業　務　仕　様　書

１　業務名

公共料金一括支払業務

２　契約期間　　契約締結日から令和 10 年 10 月 31 日まで

サービス利用期間　　令和７年 11 月１日から令和 10 年 10 月 31 日まで

（長期継続契約適用）

３　業務場所

高知市役所出納課

４　委託業務の目的

納付書等により個々に支払している携帯電話料金や電信回線料金等（以下「通信料金等」という。）の支払事務について，集約・外注化を行うことにより，事務の効率化を図るものである。

５　委託業務の概要

本業務は，令和６年４月１日に一部改正された地方自治法第 243 条の２第１項に規定されている「指定公金事務取扱者制度」により支払事務を委託するものである。

業務の概要は次のとおり。

(1) 発注者からの依頼により，各通信事業者から発注者宛に送付される請求書を「指定公金事務取扱者」の指定を受けた受注者が集約する。

(2) 受注者は，集約した通信料等を各通信事業者へ支払いを実施。

(3) 受注者は，支払した通信料金等の集約内容を CSV データ又はテキストデータで，また，支払いしたことが確認できる報告書（以下「報告書等」という。）を発注者に送付する。

(4) 発注者は，受注者から送付された報告書等の内容を確認。

(5) 報告書等の確認を受けた後に，受注者は，１カ月分をまとめて各通信事業者へ支払した通信料金と公共料金一括支払業務委託契約（以下「本契約」という。）に基づく委託料を発注者に請求する。

(6) 発注者は，受注者からの請求に基づき，支払いを実施。

6　一括支払に必要な要件

(1)　一括支払の対象

発注者から依頼された，次の通信事業者の通信料金等を対象とする。

ア　西日本電信電話株式会社

イ　ソフトバンク株式会社

ウ　ＮＴＴコミュニケーションズ株式会社

エ　株式会社ＮＴＴドコモ

オ　ＮＴＴファイナンス株式会社

カ　ＫＤＤＩ株式会社

(2) 発注者の支払処理

ア　受注者は集約した通信料金等を各通信事業者へ支払した後，その支払内容のデータと各通信事業者へ支払いした内容を確認することができる報告書を支払対象となる通信料金等が発生した月（以下「利用月」という。）の翌々月の５日までに発注者に提出すること。

ただし，年度末（３月利用分）の報告書等の提出については別途発注者と協議し，その指示に従うこと。

イ　発注者は提出されたデータと報告書の内容を速やかに確認，検査すること。

ウ　受注者は，発注者によるイの検査に合格した後，本契約に基づく委託料及び受注者が各通信事業者に支払った通信料金等を，利用月の翌々月の 10 日までに紙又はデータで請求すること。

なお，請求書をデータで提出する場合は６のウのとおりとする。

エ　発注者は適正な請求書を受理した後，毎月 20 日までに支払うこと。

(3) 一括支払に係るデータ提供要件

ア　請求データ形式

(ｱ) CSV データ又はテキストデータであること。

(ｲ) 発注者のシステムで取込処理を行うため，通信事業者を区別せず統一されたデータフォーマットであること。通信事業者により異なるフォーマットであってはならない。

(ｳ) 発注者のシステムへの取込処理に必要となる調整に応じられること。

(ｴ) データフォーマットを変更する場合は，変更を予定する前年度の９月までに情報を提供し，予め発注者と協議して行うこと。

イ　データの内容

(ｱ) 請求単位に付された番号（電話番号や請求番号等）はユニークであることとし，他と重複しないようにすること。

(ｲ) 請求単位に付された番号ごとの利用料金の明細が分かるデータであること。

ウ　請求書をデータで提供する場合の提出方法及び保存等

(ｱ) 請求書は受注者がインターネット上で提供するＷｅｂサイト等（以下「Ｗｅｂサイト」という。）から，発注者がダウンロードを行う方法又は受注者からの電子メール等による電子的な手法での提供でも差し支えない。

(ｲ) Ｗｅｂサイトへのアクセスを含め，請求データは第三者等に漏洩することのない厳重な情報管理がされていること。

(ｳ) Ｗｅｂサイトを利用する場合，受注者は，発注者に当該Ｗｅｂサイトの利用マニュアルを提供すること。当該マニュアルは紙又は発注者が読み込みできる形式の電子データにより提供するものとし，既存の資料等でも差し支えないが，内容について発注者からの問い合わせがある場合は，適切かつ丁寧な説明を行うこと。

(ｴ) Ｗｅｂサイトを利用する場合，受注者は，発注者に請求データの取得，閲覧，分析を行える権限を持つユーザーＩＤを発行すること。

7　一括支払業務に係る委託料の見積もり条件

(1) 通信回線数

通信回線数は，200 回線／月で見積すること。

※委託料はサービス利用期間開始日から発生するものとし，準備期間は含まない。

※月額利用料以外の経費がかかる場合は，契約期間の 36 カ月で割った金額を月額に加算して計上すること。

(2) 対象事業者

上記６（1）に掲げる通信事業者の請求書に対応すること。

8　一括支払業務に係る事前調整対応及び業務開始後のサポート

契約期間中において，受注者は次に掲げる内容や上記６の要件を満たすための対応を適切に行うものとする。

ア　通信事業者に支払った内容を，発注者のシステムに取り込むためのデータフォーマット案の提供や調整。

イ　対象となる通信料金等に係る請求書等の事前収集。

ウ　Web サイトの準備等，初期データの導入及び業務開始後のサポート（いずれも現地対応含む）

エ　請求内容に疑義が生じた場合，発注者からの問い合わせ等に速やかに対応すること。

オ　受注者は，集約し支払った各通信事業者の通信料金等の証拠書類について契約終了後１年間は適切に保管すること。

9　監督及び調査

(1) 監督

本契約の適正な履行を確保するため必要と認められる場合は，市担当職員を本契約のサービス提供場所，その他必要な場所に派遣し監督を行うことができるものとする。

(2) 調査

受注者は，市担当職員の質問，検査及び資料の提供などの指示に応じ，かつ，修正又は再設定の要求があったときは，これに応じなければならない。

10　情報セキュリティ管理

本契約の実施に際し，個人情報取扱特記事項を遵守するとともに，個人情報等の管理を適正かつ厳格に行うこと。

また，本契約に携わる者は，いかなる場合においても業務（付随的業務を含む）の遂行を通じて知り得た情報をもらしてはならない。その職を退いた後も同様とする。

なお，再委託を行った場合は，当該再委託先についても同様とする。

11　契約終了時の情報提供

本契約の終了後，本契約の対象となっていた通信料金等については，後継となる同様のサービスを提供する事業者に引き継ぐことを予定している。

後継サービスを提供する事業者への引継ぎのため，受注者は，発注者が本契約に基づき受注者に提供した納付書等のコピー（ＰＤＦによる電子的な提供で差し支えない）や，上記６（3）に掲げるデータ等，後継サービスを提供する事業者への引継ぎに必要となる情報について，発注者の求めにより誠実かつ確実に提供すること。

なお，当該情報の提供に係る費用は，受注者の負担とする。

12　その他

(1) 疑義の解決

受注者は，この仕様書に定める事項に疑義が生じた場合又はこの仕様書に定めのない事項で必要が生じた場合は，発注者に協議してその指示を受けること。

(2) その他

受注者は，上記６（1）に掲げる通信事業者以外の支払事務についての集約・外注化の対象範囲の拡大について，発注者の求めに応じて協力すること。

(3) サービス要件

受注者は，別紙のサービス要件を遵守すること。

別紙

サービス要件

乙は，以下の事項について基本契約又はサービスレベル契約（SLA）で定めること。

1　基本事項

（ア）日本の裁判管轄，法令が適用される。海外への機密情報の流出リスクを考慮し，外部サービスを提供するリージョン（国・地域）を国内に指定する。国内の外部サービスにおいて，利用者のデータが，海外に保存されないこと。

（イ）外部サービスの中断時の復旧要件。

（ウ）外部サービスの終了又は変更時における事前の通知等取り決めや情報資産の移行方法。

（エ）稼働率，目標復旧時間，目標復旧ポイント，バックアップの保管方法などの可用性に関する事項。

（オ）外部サービス提供者は，利用者の情報資産へ目的外のアクセスや利用を行わないこと。

（カ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制について，公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）を甲へ提案すること。

（キ）外部サービス提供者若しくはその従業員，再委託又はその他の者によって，利用者の意図しない変更が加えられないための管理体制について，公開資料や監査報告書（又は内部監査報告書・事業者の報告資料）を甲へ提案すること。

（ク）情報セキュリティインシデントへの対処方法について，外部サービス提供者との責任分担や連絡方法を取り決めること。

（ケ）脅威に対する外部サービス提供者の情報セキュリティ対策（なりすまし，情報漏えい，情報の改ざん，否認防止，権限昇格への対応，サービス拒否・停止等）の実施状況やその他契約の履行状況の確認方法。

（コ）情報セキュリティ対策の履行が不十分な場合の対処方法。

（サ）外部サービス提供者により，利用規約，各種設定が変更される可能性があるため，変更内容の確認方法や連絡方法。

2　導入・構築時のセキュリティ対策

（1） アクセス制御に関する事項

（ア）不正なアクセスを防止するためのアイデンティティ管理（ID のプロビジョニングから廃棄まで）とアクセス制御を実装すること。

（イ）システム管理者等の特権アカウントが外部サービスに接続する際は，強化された認証技術（多要素認証）を用いること。

（ウ）外部サービスに影響を与える操作の特定と誤操作を抑制するために，手順書の作成や誤操作を認識可能なアラート等の実装を考慮すること。

（エ）外部サービス上で構成される仮想マシンに対して適切なセキュリティ対策を行うこと。

（2） 暗号化に関する事項

（ア）取り扱う情報の機密性に応じた保護のための適切なアルゴリズム（CRYPTREC により安全性及び実装性能が確認された「電子政府推奨暗号リスト」）を用いた暗号化処理（情報が保存されている場合，情報が通信され転送されている場合等フローに応じた暗号化）を行うこと。

（3） 設計・設定及び開発に関する事項

別紙

（ア）外部サービス利用の企画，要件の確認の段階から想定される脅威やリスクに対するセキュリティ対策を検討し，その検討結果を踏まえ，設計・開発におけるセキュリティ対策を行うこと。
また，外部サービスで取得可能なログの種類，範囲等を確認し，必要となるログの取得機能を実装すること。

（イ）外部サービス内における時刻同期の方法について確認し，取得するログの時刻，タイムゾーンを統一すること。

（ウ）設計・設定時の誤りの防止の対応として，設計書や設定のレビューやクラウドサービスのフレームワークとの比較などを行うこと。

（エ）乙は，セキュリティを保つための開発手順やフレームワーク等の情報を活用し，甲へ提案すること。

（オ）外部サービス上に他ベンダーが提供するソフトウェア等を導入する場合は，そのソフトウェアの外部サービス上におけるライセンス規定を確認すること。

（カ）外部サービス上に構成された情報システムと他の外部サービス利用者のネットワークやサブネット間等の異なるネットワーク間の通信（トラフィック）を監視すること。

（キ）利用する外部サービス上の情報システムが利用するデータ容量や稼働性能（移植容易性）について，業務が継続できるよう考慮すること。

（ク）可用性（冗長構成や場長回線等の実装）を考慮した設計とすること。

3　運用・保守のセキュリティ対策に関する事項

（1） 利用方針に関する事項

（ア）外部サービス提供者は，責任分界点について明確にすること。

（イ）利用するサービスに係る情報セキュリティインシデント発生時の連絡体制を明確にすること。

（2） 教育に関する事項

（ア）サービスの手順書（操作手順書）を作成し，甲へ提案すること。

（3） 資産管理に関する事項

（ア）情報資産の責任範囲を明確にすること。

（4） アクセス制御に関する事項

（ア）必要に応じてシステム管理者特権を割り当てる場合のアクセス管理と操作に関するログを取得すること。

（イ）必要に応じて各利用者に割り当てたアクセス権限に対して，定期的な見直し（異動時，退職時等の確認）を行うこと。

（ウ）リソース設定を変更するユーティリティプログラムを使用する場合は，必要に応じてその機能の確認と利用できる者を制限すること。

（エ）不正な利用を監視（例：業務時間外の利用等を外部サービスに対するアクセスログで確認）できるようにすること。

（5） 暗号化に関する事項

（ア）暗号化の仕組みや暗号化に使用する鍵の管理方法について提案し，甲の承認を得ること。

（イ）鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みに関する内容を確認し，リスクがないことを確認すること。

別紙

（6） 外部サービス内の通信に関する事項

（ア）ネットワーク基盤が他の利用者のネットワークや通信と分離されていることを確認し，甲へ報告すること。

（7） 設計・設定に関する事項

（ア）設定を変更する場合，設定の誤りを防止するための対策（グローバルなセキュリティのガイドラインやフレームワークとの差異の確認等）を行うことができるようにすること。

（イ）利用者が行う重要な操作に関する手順書を作成し，甲に提案すること。

（ウ）仮想マシンのネットワークが他の利用者のネットワークと分離されていることを確認し，甲へ報告すること。

（8） 事業継続に関する事項

（ア）不測の事態に対してサービスの復旧を行うために必要なバックアップを実施（外部サービス提供者が提供する機能を利用する場合は，その実施の確認）すること。

（イ）業務に必要な可用性を満たすことを確認し，復旧に係る手順の策定と定期的な訓練について甲と協議すること。

（ウ）設定やバージョン等の変更の確認方法とシステムに影響があった場合を想定し，復旧手順を甲と協議すること。

（エ）データの容量，性能等を監視し，サービスまたはサービス上のシステムへの影響について把握できること。

（9） インシデント対応に関する事項

（ア）甲が情報セキュリティインシデントや情報の目的外利用等を認知した場合，外部サービス管理者へ報告できるようにすること。

（イ）インシデント報告を受けた場合の対応手順を定めること。

4　更改・廃棄時のセキュリティ対策に関する事項

（1） 利用終了時における対策に関する事項

（ア）外部サービスの利用を終了する場合は，必要に応じて移行計画書又は終了計画書を作成すること。

（イ）外部サービスの利用終了による業務影響が無いように，利用者に対して利用終了の予定時期を事前に知らせること。

（2） 情報の廃棄に関する事項

（ア）取り扱う情報の機密性に応じて，廃棄方法を甲に提案すること。

（3） アカウントの廃棄に関する事項

（ア）各アカウントを削除できること。

（イ）管理者特権アカウントを削除（又は返却）できること。

（ウ）特殊なアカウントがある場合は，関連情報（資格情報等）含めて廃棄できること。

5　利用状況の管理

（ア）利用している外部サービスについて，定期的な確認を行い，甲から確認があった場合に提示できること。内容に変更があり，不適切と考えられるものがある場合は，甲と協議すること。

別紙

６　クラウドサービスの利用に関する事項

（ア）マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については，マイナンバー利用事務系として扱い，甲の他の領域とはネットワークを分離すること。

（イ）LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は，その領域を LGWAN 接続系として扱い，マイナンバー利用事務系とネットワークを分離し，専用回線を用いて接続すること。

（ウ）パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合，その管理手順が，甲が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすこと。