「電子申請・届出システム手数料等キャッシュレス決済（コード決済等）業務委託」仕様書

本仕様書は、茨城県（以下、「県」という。）が、いばらき電子申請・届出サービス（以下、「電子申請・届出システム」という。）を用いて申請者から歳入等の納付を受託する業務について、その業務の範囲及び条件等を定めるものである。

第１　業務名

電子申請・届出システム手数料等キャッシュレス決済（コード決済等）業務

第２　目的

電子申請・届出システムにおいてコード決済等の新たな決裁機能を導入し、利用者の利便性の向上を図る。

第３　契約期間

契約を締結した日から令和９年９月 30 日まで

ただし、翌年度以降の歳入歳出予算におけるこの契約に係る金額について、減額又は削除があった場合は、契約を解除できる。

第４　本業務の対象及び取扱範囲

（１）本業務の対象システム

電子申請・届出システム

（２）本業務で納付する手数料等（第５以降において「手数料等」とする。）

前項のシステムにおいて発生した各種手続における申請手数料、受講料、購入代金等全ての支払い

第５　対象となる決済サービス及び利用開始予定日

以下について決済が可能であること。

なお、Pay-easy 及びクレジットカードは導入済のため、提案内容から除くこととする。

	決済サービス	利用開始予定日
1	PayPay	令和７年 10 月１日
2	d 払い	令和７年 10 月１日
3	au PAY	令和７年 10 月１日
4	楽天ペイ	令和７年 10 月１日
5	コンビニ決済（番号方式）	令和７年 10 月１日

第６　取扱予定件数及び取扱予定金額

第５に示す決済サービスによる取扱予定数量は次の通りである。

なお、当該数量はあくまで見込みであり、実際の取扱件数及び取扱金額とは異なる。

期間	取扱件数	取扱金額
令和７年 10 月１日～令和８年３月 31 日	2,500 件	36,000 千円
令和８年４月１日～令和９年３月 31 日	7,500 件	108,000 千円
令和９年４月１日～令和９年９月 30 日	7,500 件	108,000 千円

第７　収納データに係る対応業務

（１）電子申請・届出システムへの収納データの連携にかかるインターフェース仕様や接続方法については、株式会社ＮＴＴデータ関西のｅ－ＴＵＭＯ　ＡＰＰＬＹ電子申請サービスが連携できることを前提とする。

（２）受託者は、県が、電子申請・届出システムの収納データを県の財務事務を処理するシステム（以下、「財務システム」という。）に取り込むために、第５に定める取扱開始予定日までに、電子申請・届出システムとの疎通試験及び一連の業務手続を通したシステム全体の確認試験等を行う。

（３）その他、電子申請・届出システム、財務システム等と連携するために必要な調整がある場合は、各団体と協力する。

第８　納付事務準備業務

受託者は、第５に定める各決済サービスの利用開始予定日までに、以下の業務を行うものとする。

（１）管理画面の維持管理運営

受託者は、以下の要件に適合した管理画面を用意する。

（ア）Microsoft Edge、Google Chrome、Safari 等の最新バージョンのブラウザで動作するものとすること。

（イ）電子申請・届出システムからの収納対象データを表示する機能を有すること。

（ウ）収納結果データを電子データ（csv 形式等）により、県に納品する機能を有すること。

（エ）県が、払込み金額の内訳に関する情報を確認する機能を有すること。

（オ）県が、個別の収納対象データの収納状況（納付番号、納付区分、納付額及び決済年月日等）を確認する機能を有すること。

（カ）県が、月次収納実績（決済日時、納付金額）を確認する機能（個々の収納データについて確認する機能）を有すること。

（２）電子申請・届出システムとのシステム連動にかかる確認

受託者は、電子申請・届出システムとの電子データ伝送を含め、本業務を履行するにあたって支障がないことを事前に確認する。

第９　納付事務業務

（１）管理画面の維持管理運営

受託者は、第８により用意した管理画面を維持管理運営する。

（ア）Microsoft Edge、Google Chrome、Safari 等の最新バージョンのブラウザで新たなバージョンがリリースされた場合は、遅滞なく対応すること。

（イ）24 時間 365 日稼働すること。但し、受託者のシステムメンテナンスなどにより全て又は一部の機能が使用できなくなる場合は、緊急時を除き事前に県に報告すること。

（２）納付事務に係る申込受付

受託者は納付画面にて、申請者から納付事務の申込みを受け付けること。24 時間 365 日稼働すること。但し、受託者のシステムメンテナンスなどにより本業務の全て又は一部を中止又は停止する場合は、緊急時を除き事前に県に報告すること。

（３）カード等の利用確認等

受託者は受け付けた納付事務の申込に係る決済サービスの利用確認等を遅滞なく行い、決済事業者から承認を得られたときは、当該申込を承諾すること。

（４）収納結果データの連携及び納品

（ア）受託者は、キャッシュレス取引が正常に完了した場合、また、取消等が正常に完了した場合、遅滞なく電子申請・届出システムに収納結果データを連携させ、電子申請・届出システム上で県が確認できるようにすること。

（イ）受託者は、毎月 1 日を起算日として 10 営業日までに、前月の申込承諾分を取り纏め、収納結果データを作成の上、県に提供すること。なお、収納結果データとして必要な項目は、県及び受託者の協議により決定するものとすること。

（ウ）受託者は、通信回線の不通（短時間で復旧すると認められる場合を除く。）又は自己のシステム機器等の不具合により、県に収納結果データを管理画面から納品、又は電子申請・届出システム上に連携できない場合は、データの漏えい、紛失、毀損及び盗難等がないよう必要な事故防止対策を講じた上で、送付できなくなったデータを、原則として、毎月 1 日を起算日として 10 営業日までに県に提供する代替手段を用意すること。

（５）払込み

受託者は、申請者から委託を受けた歳入等を第 10（２）に示すスケジュールに沿って県に納付する。

第 10　収納金の送付業務

（１）受託者は、地方自治法第 231 条の２の３第１項の規定による指定納付受託者となること。

（２）キャッシュレス決済の収納金の送金は、毎月毎に末日を締日として集計し、翌月 15 日までに、県が指定する口座に振り込むこと。ただし、15 日が金融機関の休業日に当たる場合は、翌営業日までとする。また、収納金の振込に係る送金手数料については受託者の負担とする。

（３）キャッシュレス決済に係る受託者の決済手数料については、受託者が発行する毎月の請求書によって、キャッシュレス決済手段や決済ブランドの種類を問わず、毎月払いで支払うこととし、徴収した収納金から決済手数料を差引したうえでの送金は行わない。
（４）決済手数料は、徴収した金額に提案書の手数料率を乗じた金額とする。なお、１円未満の端数があるときは、原則としてその端数は切り捨てるものとする。
（５）コンビニ決済に係る決済手数料は、前項の規定に関わらず、徴収した金額に応じた手数料とする。

第 11　機器の設置等費用負担

受託者が本業務の履行に際して必要とする機器等（コンピュータソフトウェアのプログラムを含む）は、次の各号の範囲を除き、受託者が用意するものとする。
（１）電子申請・届出システム
（２）電子申請・届出システムと受託者のシステム機器等の間で収納対象データを伝送するための電気通信回線
（３）県が管理画面を閲覧するために必要となる業務用端末及び電気通信回線

第 12　問合せ及び苦情等の対応

（１）本業務に関する申請者等からの問合せについて、県から受託者に問合せがあった場合は、受託者は迅速に対応するものとする。
（２）受託者は、設置する問合せ窓口に寄せられた質問、苦情等のうち県に起因するものであると判断する場合には、問合せをした者に対してその旨を回答すると共に、県に対して直近の営業日に応対結果を通知するものとする。
（３）県及び受託者に起因する質問の場合等は、協力してこれを解決するものとする。

第 13　業務計画書

受託者は、第６に掲げた利用開始予定日を前提として、第７から第９に掲げた業務内容に係る作業工程（通信接続試験等を含む）を県へ提出する。

ただし、開始時期を変更する場合には、県及び受託者間で別途調整する。

第 14　障害対応

（１）収納データに係るサーバ等重要な機器を堅牢なデータセンターに設置し、冗長化（二重化等）するなど、大規模災害などに対しても信頼性の高いシステムを導入し、障害発生時に早急な復旧が可能な状態にすること。
（２）システム障害等により収納データが提供できない事象が生じた場合、受託者は、直ちに県に報告するとともに、早急に復旧へ向けた対応を行うこと。
（３）復旧対応中は対応経過を随時報告すること。
（４）復旧後、収納データの提供が可能となった際には、直ちに県に報告すること。また、障

害等の原因及び影響を調査し、再発防止策を講じるとともに、その結果を遅滞なく県に報告すること。

第15　情報セキュリティ対策

（1）受託者は、以下のセキュリティ対策を講じること。

- 通信経路上での暗号化（SSL等）
- ウィルス対策ソフトの導入及びパターンファイルの定期的な更新
- セキュリティパッチの定期的な適用
- ID及びパスワード等によるユーザ認証等
- その他、必要なセキュリティ対策

（2）不正侵入やデータの改ざん等の不正アクセス防止に対する万全のセキュリティ対策を講じること。