船橋市防犯灯設置管理業務　システム仕様書

1　適用

この仕様書は、「船橋市防犯灯設置管理業務　仕様書」に定めるもののほか、防犯灯管理システムに関して必要な事項を定める。

2　業務内容（以下「本業務」という。）

⑴　システム構築
⑵　システム導入作業
⑶　システム維持管理
⑷　システム保守

3　防犯灯管理システムの要件

⑴　概要

①　市内約 48,000 灯の防犯灯等の照明を管理できるようにすること。
②　市内に所在する防犯灯等の位置や設置状況を把握するため現地調査を行い、その結果をシステムに反映させること。
③　現地調査の対象とする防犯灯等については、業務仕様書に定めるとおりとする。
④　システム稼働時間は、原則 24 時間 365 日とする。ただし、システム停止が必要なバックアップ時及び定期保守点検時を除く。
⑤　契約履行期間中、灯数の増減やデータ内容に変更があった場合は、市の承認を得た上で、市が指定した時期までにシステムに反映させること。
⑥　利用者は、市の担当部署のほか、事業者、コールセンター及び市の担当部署以外の庁内部署を想定している。
⑦　システム利用時は、ID 及びパスワードを入力してログインするよう設定すること。なお、ID 及びパスワードの付与権限については、市と事業者が協議して決定すること。

⑵　必要条件

①　日本の法令の範囲内で運用できるサービスであること。また、日本国内の裁判所を合意管轄裁判所とすること。
②　個人情報や住民の生命・財産に関わる情報、その他非公開情報のデータが保存されるデータセンターは日本国内にあること。

③　利用するクラウドサービスのリージョンを日本国内に限定すること。
④　脅威に対するクラウド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を盛り込んだ契約が締結可能なこと。
⑤　クラウドサービス提供者における情報セキュリティ対策が確実に実施されること。

⑶　性能

①　事業者がシステムを構築し、データセンターにおいて運用管理され、インターネットを経由して提供されるクラウドサービスであること。
②　業務継続性を確保するため、汎用性の高いデータベースやソフトを用いて構築すること。
③　市で使用できるアカウント数（ライセンス数）は、少なくとも 30 件確保するものとし、同時接続が可能となるようにすること。その他、コールセンター等で必要となる数も確保すること。
④　利用者数が最大となった場合においても、機器の増設が無く許容できる処理性能を有していること。
⑤　利用時に処理速度が低下せず、ストレスなく利用できるレスポンスを有すること。
⑥　システムに求める機能は、別紙機能一覧のとおりとする。なお、詳細については、市と事業者が協議して決定する。

4　業務実施体制

⑴　事業者は、本業務の実施に当たり、業務の統括、担当者の指揮監督、市との連絡調整等にあたる業務責任者を選任すること。業務責任者は、システム及び業務について熟知した者から選任すること。なお、業務責任者については契約時に市に報告すること。
⑵　事業者は、市との十分な連携及び意思疎通を図りながら、効率的かつ効果的な業務実施体制を構築するとともに、円滑な運営のため適宜打合せを行うこと。なお、打ち合わせ後は、事業者において議事録を作成し、市の承認を得ること。
⑶　クラウドサービスの開発及び運用について、市の意図しない変更が行われない一貫した品質保証体制の下でなされていること。なお、意図しない変更とは、非公開設定が説明なく公開設定になることや、市が保存するデータが意図せず書き換えられること等を想定しており、機能追加等はこれに含まれない。
⑷　システムの更新にあたっては、プロジェクト管理（品質及び進捗管理）を行うこと。

5　システム導入

⑴　事業者は、契約締結後、システム導入までの業務計画書（スケジュール等）を提出し、市の了承を得ること。

⑵　事業者が管理するサーバ環境（データセンター）にシステムを構築するとともに、ソフトウェア等をインストールし、必要な調整作業を実施する。

⑶　システム導入時の設定及び初期調整作業は、事業者の責任にて対応すること。

⑷　システム構築の際、市利用環境は、市端末で利用できること。なお、市端末は以下の環境とする。市利用環境に変更が生じた場合は、変更内容に合わせて対応すること。

パソコン（Windows11／Microsoft Edge（IE モード使用不可）、Google Chrome）

※本市の既設パソコンは内部ネットワークとインターネットを分離しており、セキュアコンテナ（ローカル環境とは独立した仮想的な環境）内のブラウザ（Microsoft Edge（IE モード使用不可）、Google Chrome）を使用してインターネットへ接続している。そのため上記インターネット接続環境にてアクセスできる環境を用意すること。

⑸　市が既に利用している庁内 WebGIS データと連携できる機能を想定し、市が指定する項目をデータで提供できるようにすること。なお、提供時のファイル形式や使用する座標系については、市と事業者が協議して決定する。

⑹　市保有のデータをシステムへ反映する必要が生じた際、対応可能な体制となるよう、データ（Shapefile 形式、csv ファイル形式等）の取込に対応できるよう努めること。

⑺　世界測地系に基づく最新の地図を用いて構築すること。なお、住宅地図を使用する場合には導入後、住宅地図データを概ね 5 年程度で更新することを想定しているが、更新時期については市と事業者が協議して決定する。

⑻　システム構築は令和 10 年 1 月末日までに完了させ、令和 10 年 4 月 1 日から本稼働すること。なお、システム構築後から本稼働までの間に、仮稼働期間を 1 か月以上確保すること。

⑼　構築したシステムについて、システムの各機能及び搭載データが正しく動作・表示されていることを確認するため、本稼働までにシステムテストを行うこと。なお、確認の対象は、システムに搭載された全機能とし、システムテスト実施に当たっては、システムテスト計画書及びシステムテスト結果報告書を市に提出すること。

⑽　市に対して、本稼働前に操作説明を実施すること。また、利用者向けの操作マニュアルを作成すること。

⑾　クラウドサービスに影響を与える操作（サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除・利用の終了手順・バックアップ及び復旧等）について、誤操作を抑制するための手順書の作成や誤操作を認識可能なアラート等を実装する等の対策を行うこと。

⑿　クラウドサービス内において確実に時刻同期を行い、取得するログの時刻、タイム

ゾーンを統一すること。

⒀　設計・設定時の誤りの防止の対応として、次の対策を行うこと。

①　クラウドサービス提供者による設定の実施

②　クラウドサービス提供者からの推奨される設定情報の入手

③　クラウドサービス提供者による設定内容のレビュー

④　クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用

⑤　設定権限を与えるクラウドサービス利用者の限定

6　再委託の禁止

本業務の一部又は全部の実施を第三者に再委託してはならない。ただし、あらかじめ書面により市の許諾を得たときは、その限りでない。

7　セキュリティ対策

⑴　システムを利用する際には、必ず SSL による暗号化処理を行い、ID 及びパスワードの入力によりシステムに認証されたもののみが利用できること。

⑵　パスワードの管理機能については、市と事業者が協議して決定する。

⑶　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提供者側で実施される場合、次の管理手順が実施されること。

①　パスワードは、他者に知られないように管理しなければならない。

②　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③　パスワードは十分な長さとし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い､数字や記号を織り交ぜる等)にしなければならない。

④　パスワードが流出したおそれがある場合には、速やかに報告し、パスワードを変更しなければならない。

⑤　サーバ、ネットワーク機器、パソコン及びモバイル端末等にパスワードを記憶させてはならない。ただし、一定のセキュリティ水準に沿った運用が担保できる場合は、市と事業者が協議して取り扱いを決定する。

⑷　利用できる機能を利用者ごとに制御ができること。

⑸　個人情報保護をシステム内で取り扱うときは、グローバル IP アドレスによるアクセス制御ができること。

⑹　システムへの第三者による不正アクセスや利用者の個人情報の漏えいを防ぐため、必要なセキュリティ対策を講じること。

⑺　高度標的型攻撃などのサイバー攻撃による不正な侵入を防止するために技術的な対策を講じること。

⑻　システムを管理するデータセンター及び事業者は、個人情報を含むデータの取扱いを想定し、市の情報資産を適切に扱うことができるようにすること。

⑼　データセンターは、日本データセンター協会が定める「データセンターファシリティスタンダード」の Tier3 相当以上であること。なお、Tier3 に満たない項目があるときは、市に協議すること。

⑽　当該クラウドサービスに関連する脆弱性情報の提供を行うこと。また、クラウドサービス提供者の責任範囲で発生した脆弱性対応が迅速に行われること。

⑾　クラウドサービス提供者が提供する鍵管理機能を利用するときは、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にリスク（鍵が窃取される可能性や鍵生成アルゴリズムの危殆化の可能性等）がないこと。

⑿　クラウド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（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策、ログ取得等の実施）を行うこと。SaaS を利用する場合は、これらの対応が、事業者側でされていること。

⒀　取り扱う情報の機密性に応じて、暗号化処理等により情報資産が適正に保護されること。

⒁　公開するウェブサイトの全てのページの通信を暗号化し、データ送信は、常時、SSL 証明書で暗号化された通信（https）により行うこと。なお、サーバ証明書は、事業者が用意し、その費用も本業務の費用に含めること。

⒂　再委託されることにより生ずる脅威に対して、情報セキュリティが十分に確保されていること。

⒃　再委託先の情報セキュリティ対策の実施状況を確認するため、次の内容をはじめとした情報を市に提供可能であること。

①　再委託先事業者情報
②　再委託内容
③　再委託先の情報セキュリティ責任者
④　再委託先の個人情報管理者
⑤　再委託先の従事者の情報

8　データ移行及び業務の引き継ぎ

本業務の契約履行期間の満了、全部もしくは一部の解除又はその他契約の終了事由の如何を問わず、本業務が終了となる場合には、事業者は市の指示のもと、本業務終了日までに市が継続して本業務を遂行できるよう必要な措置を講じること。また、業務引き継ぎに伴うシステム移行等に必要となる構成要素を円滑に提供できるようにすること。なお、移行用のデータ提供に係る費用は、本契約に含まれるものとして取り扱うこと。

9　業務履行状況調査

市は、事業者に対して、常時、本業務履行状況に関する調査（立入調査含む）を行うことができるものとする。

10　納品物

納品物及び提出時期は、次の表のとおりとする。

納品物	提出時期
業務計画書（スケジュール等）	契約締結後、速やかに
要件定義書	契約締結後、市が定める日まで
基本設計書	
詳細設計書（パラメータシート）	
システムテスト計画書	システムテスト開始前まで
システムテスト結果報告書	システムテスト完了後、速やかに
サーバ及びシステム構成図	システム本稼働前まで
操作マニュアル	本稼働前の操作説明時まで
業務完了報告書	業務ごとに市と協議して決定

11　危機管理体制の確保

⑴　事業者は、常にサービスの向上と効率化の確保に向けた仕組みを整備するとともに、トラブルの未然防止対策やトラブルが発生したときの危機管理体制を確保すること。

⑵　事故等が発生したときには、直ちに市に報告するとともに、必要な措置を講じること。また、その発生原因が事業者側にあるときは、事業者が責任を持って適切に対処し、速やかに事故報告書を市に提出すること。

⑶　情報セキュリティインシデントが発生した際に、事業者と連絡がつかない状況や、営業時間外の対応が不可能等の状況にならないこと。また、情報セキュリティインシデントによる被害を最小限に食い止めるため、情報セキュリティインシデント発生時に次の対応を行うこと。

①　情報セキュリティインシデントを検知したときは､速やかに市に報告を行うこと。

②　情報セキュリティインシデントが発生したときは、運用状況・影響範囲調査等、事案解決のために積極的に調査を行うこと。

③　情報セキュリティインシデント発生後、速やかに調査に着手すること。また、情

報セキュリティインシデントの疑いに対する連絡を受けた場合も同様とする。なお、調査着手までの時間は、市と事業者が協議して決定すること。

④　情報セキュリティインシデントの原因特定のため、各種システムログを取得すること。また、取得したログの分析に必要な情報を提供すること。

⑤　調査の結果、サービス停止等の措置が必要な場合は、市に報告した上で速やかにその対応を行い、インシデント収束後、速やかに復旧を行うこと。

⑥　調査の結果、ファームウェア・ソフトウェア等のバージョンアップ等が必要となった場合は、速やかに対応すること。

12　機密保持及び情報セキュリティの確保

⑴　事業者は、本業務に関連して知り得た船橋市の機密に関する事項及び個人情報に関する事項については、「個人情報の保護に関する法律」、「船橋市個人情報の保護に関する法律施行条例」、「船橋市情報セキュリティ基本方針」及び「船橋市情報セキュリティ対策基準」等に基づいて適切に管理し、契約期間中はもとより、契約期間後も第三者に漏えいしてはならない。

⑵　事業者は、市の許可なく個人情報等（機密情報を含む）の情報資産を持ち出してはならない。

⑶　個人情報等（機密情報を含む。）の情報資産の授受は、市の指定する方法により、市の指定する職員と事業者の指定する者の間で行うものとする。

⑷　特定個人情報を取り扱う場合は、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）」に記載のある安全管理措置に基づいた措置を講じること。

⑸　クラウドサービス提供者による情報資産の利用は、クラウドサービスの提供に必要な範囲で認めるものであり、それ以外の目的で市の情報資産の利用は認めない。

⑹　クラウドサービスの利用終了時に、クラウドサービスで取り扱った業務に関わる全ての情報が、クラウドサービス基盤上から確実に削除可能であること。なお、削除する対象は、バックアップ等により複製されたものにも及ぶ点に注意し、削除に当たっては、情報資産を暗号化した鍵（暗号鍵）を削除するなどにより、復元困難な状態としなければならない。

⑺　クラウドサービスの基盤となる装置等の処分についてセキュリティを確保した対応が行われること。

⑻　クラウドサービスの利用終了時に、情報の廃棄の実施報告書を提出すること。

⑼　クラウドサービス利用者の各アカウント以外に特殊なアカウント（ストレージアカウント等）がある場合は、関連情報（資格情報等）含めて廃棄可能であること。

13　関係法令等の遵守

事業者は、本業務の実施にあたり、労働基準法、労働安全衛生法、最低賃金法、地方公務員法その他関係法令等を遵守すること。また、市が定める関係条例等を遵守し、適法かつ適切な業務を遂行すること。

14　権利の帰属

システムで取り扱う全てのデータに関する所有権は、市に帰属するものとする。

15　運用保守等の要件

⑴　システムに係る維持管理及び保守の体制が継続して提供可能であること。
⑵　市からの問合せに対応できる体制を整備すること。また、対応が可能な時間は、祝日及び事業者規定の定休日を除いた月曜日から金曜日までの午前 9 時から午後 5 時までとする。ただし、緊急時はこの限りでない。
⑶　システムの運用過程で障害が発生した場合は、速やかに原因を調査し修復すること。
⑷　保守対応時間帯以外に、サーバ及びサービス監視（リモート）を 24 時間 365 日行い、異常が発見されたときは、翌営業日に初動対応を行い、2 営業日以内に復旧すること。また、サーバ及びサービス監視（リモート）において、アラート発生の条件が適切でないと判断する場合、条件設定を適時見直し、不要なアラート発生を防ぐものとする。
⑸　データセンターでは、有人による入退室管理が行われているものとし、トラブルに備え、保守要員を配置すること。なお、保守要員の対応時間については、市と事業者が協議して決定すること。
⑹　システムの安定稼働のため、サーバには無停電電源装置（UPS）及び非常用発電設備により、無停電で電源を供給できること。
⑺　データのバックアップは毎日行い、日次で 7 世代保管すること。また、フルバックアップを少なくとも年次で行い、事業者にて保管すること。
⑻　システムの OS やソフトウェアについて、月に 1 回、セキュリティパッチを適用すること。
⑼　システム稼働後、システムに改良、追加等の必要が生じた場合には、事前に市と事業者が協議して速やかに対応すること。なお、この対応に関する費用負担については、市と事業者が協議して決定すること。
⑽　システムの利用規約に変更が生じるときは、1 か月前までに書面又は電磁的方法にて市に告知すること。

⑾　クラウドサービスに係るログ等の証跡の保存、取得及び提供が可能であり、ログは少なくとも１年以上保存すること。また、改ざん防止等のログ等に関する保護が実施されていること。

⑿　クラウドサービスの設定を変更する場合、次の設定の誤りを防止するための対策を行うこと。

①　クラウドサービス提供者による設定の実施

②　クラウドサービス提供者からの推奨される設定情報の入手

③　クラウドサービス提供者による設定内容のレビュー

④　クラウドサービス提供者が提供するセキュリティ設定・監視ツールの利用

⑤　設定権限を与えるクラウドサービス利用者の限定

⑥　追加機能に対する初期設定や追加機能により影響を受ける設定の確認

⒁　システムで使用するクラウドサービスの終了または変更の際は、6 か月前までに書面又は電磁的方法で告知すること。なお、クラウドサービスが終了する場合には、代替のクラウドサービスについて市に提案し、許諾を得ること。

16　特記事項

⑴　本業務に必要な機械及び設備は、市の許可を受けた上で使用すること。

⑵　契約終了後、システムの利用については、市と事業者が協議して、継続利用できるようにすること。