別紙3　情報セキュリティ対策要件

No.	対策要件	実施する対策
1	通信経路の分離	不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、本市ネットワーク内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。
2	不正通信の遮断	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルやアプリケーションの通信を通信回線上にて遮断する機能を備えること。
3	通信のなりすまし防止	情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えること。
4	サービス不能化の防止	サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。
5	マルウェアの感染防止	マルウェア（ウイルス、ワーム、ボット等）による脅威に備えるため、想定されるマルウェアの感染経路の全てにおいて感染や感染拡大を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。
6	構築時の脆弱性対策	情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。
7	運用時の脆弱性対策	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施し、情報システム全体の更新漏れを防止する機能または運用を備えること。また、調達機器において、緊急度が高く保守対象の運用に影響を与える可能性が高いと考えられる脆弱性が発生した場合は、発注者と協議の上、機器の稼働に影響が無い範囲で当該脆弱性を解消する支援を行うこと。
8	ログの蓄積と管理	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、１週間以上保管すること。
9	ログの保護	ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。
10	時刻の正確性確保	情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
11	侵入検知	不正行為に迅速に対処するため、通信回線を介して所属する本市外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。
12	主体認証	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち本システムを利用する道路管理者の認証を行う機能として、ID/パスワード認証の方式を採用すること。
13	ライフサイクル管理	主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。
14	管理者権限の保護	特権を有する管理者による不正を防止するため、管理者権限を制御する機能又は運用を備えること。

15	情報の物理的保護	情報の漏えいを防止するため、庁舎外使用時にはスマートフォンの紛失等がないよう各職員が厳格に管理を行うこと。また、盤への施錠等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。
16	侵入の物理的対策	物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。
17	システムの構成管理	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに、文書どおりの構成とすること。
18	システムの可用性確保	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が目標復旧時間として48時間（営業日以外を除く）を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。
19	委託先において不正プログラム等が組み込まれることへの対策	情報システムの構築において、本市が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。
20	調達する機器等に不正プログラム等が組み込まれることへの対策	機器等の調達工程において、本市が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。
21	情報セキュリティ水準低下の防止	情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。
22	プライバシー保護	情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者から意図しない形で第三者に送信されないようにすること。