別紙２

情報セキュリティ要件

１　クラウドサービス提供者が ISO/IEC27001 認証を取得していること。

２　定期保守のためサービスを停止する場合は 30 日前に本市へ事前連絡を行うこと。
また、臨時的な保守のためサービスを停止する場合は１日前に事前連絡を行うこと。

３　サービスの提供時間は 24 時間 365 日とすること。（計画停止/定期保守を除く。）

４　サービス稼働率は 99.5%以上とし、システム停止を伴う障害発生回数は年２回以内とすること。

５　業務停止を伴う障害が発生した場合、その旨を速やかに本市に通知し、本市と協議したうえで速やかに対応すること。

６　すべてのデータに対して日次で差分バックアップ、週次でフルバックアップを行い、４世代まで保持すること。

７　クラウドサービスで取り扱うデータ（バックアップデータを含む。）の所在地を日本国内に限定すること。

８　準拠法、裁判管轄は国内とすること。

９　本市が登録したデータは、本市に確実に提供でき、提供後のデータの所有権・管理権は、市が保有すること。また、当該データは契約に明示的に定められているところを除き、本市の承諾なく、利用しないこと。

10　本市が取り扱う情報について、クラウドサービス提供者においてクラウドサービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用しないこと。

11　クラウドサービスの提供にあたり、クラウドサービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制を整備すること。

12　クラウドサービス提供者はその作業内容を一部再委託する場合は本市の承諾を得ること。

13　クラウドサービス提供者がその作業内容を一部再委託する場合は、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るよう担保すること。

14　情報セキュリティインシデントが発生した場合に備え、事前に対応手順書を作成し、本市に提出すること。

15　提出された手順書に基づき、インシデント発生時には本市と連携しながら適切に対応を行うこと。

16　上記対応後は、原因分析と再発防止策の実施したうえで報告を行うこと。

17　アクセスログや操作ログなどの必要なログの種類について、取得機能を実装し、最低１年間以上の期間、ログの保存が可能であること。

18　ログについて、下記のいずれかの対応が可能であること。

・本市が必要とする場合に、閲覧や提供が可能であること。
・本市の依頼に応じて調査し、調査結果を本市に報告すること。

19　データの通信について、TLS 1.2 以上のプロトコルを用いて通信の暗号化を行うこと。

20　データそのものについて、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の「電子政府推奨暗号リスト」で推奨された暗号を用いた暗号化処理を行うこと。

21　消防団員側は、利用者 ID によるアカウント設定が可能で、これらのアカウントについては本市の職員が管理権限を持つこと。職員側は、ID およびパスワードによるアカウント設定が可能であること。

22　通信内容を監視し、不正アクセスや不正侵入を検知・通知できる仕組みを導入し、リアルタイムで異常を検知・対応できること。

23　アクセス端末や IP アドレスによるアクセス制御機能を備え、許可された端末や IP アドレスからのみアクセスを許可することに加え、二段階認証（メール認証、コード認証など）でのアクセスが可能であること。

24　クラウドサービス上の脆弱性について常に最新情報を収集し、脆弱性が確認された場合は、本市に報告のうえ迅速な対応を行うこと。

25　クラウドサービスの利用終了時には、業務で取り扱うすべての情報（ログ情報を含む）を、適切に消去または廃棄すること。

26　下記の内容が確認できるデータ消去に関する証跡文書を本市に提出すること。
・消去した情報
・データ消去作業の実施日
・消去作業を実施した担当者の氏名または部署名
・その他、消去作業を実施したことが確認できる情報