別紙１

情報セキュリティ要件

１．受注者は、情報セキュリティ要件を予め確認し、再委託先がある場合は再委託先も含めて、情報セキュリティ要件を遵守できることを確認した上で入札または見積書の提出を行うこと。

また、発注者が定める「情報管理体制図」及び「情報セキュリティ要件遵守報告」を、袋井市役所の本事業担当職員に契約締結前と事業終了時に根拠資料とともに担当職員に提出すること。

なお、報告の内容について、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

加えて、事業実施期間中にこれらに変更が生じる場合は、事前に担当職員へ案を提出し同意を得ること。

２．受注者は、本業務を再委託する場合は、再委託先においても本セキュリティ要件を遵守するよう再委託先を指導し、遵守状況の確認を行うこと。

また、本業務を再委託する場合は「情報管理体制図」には再委託先の従事者等を含めること。

３．受注者は、本業務遂行中に得た本業務に関する情報の取扱いには十分注意を払い、漏洩を防ぐこと。

受注者は、サービスを終了または契約終了する際には、予め定めた方法によってサービス上のデータの移管及び消去を行うとともに、受注者においては本業務遂行中に得た本業務に関する情報を速やかに消去すること。

なお、サービス上のデータの移管及び消去に関して発注者側で行う場合は、受注者はその方法を提示し、確実な消去を行えるようにすること。

消去を実施した旨を、事業終了時に「情報セキュリティ要件遵守報告」に記載して提出すること。

受注者は、契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

４．受注者は、本業務で利用した機器を廃棄する場合は、予め定めた方法でデータの移管及び消去を行うとともに、機器内のデータを復元不能な状態で廃棄し、事業終了時に「情報セキュリティ要件遵守報告」に記載して提出すること。

５．受注者は、本業務で提供するクラウドサービスおよび本業務で使用するソフトウェア、電子計算機等について、脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じること。

加えて、これらの対策を含め情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

６．受注者は、本業務に従事する者を限定し、従事する者の氏名、所属、専門性、国籍、連絡先をまとめた「情報管理体制図」を担当職員に提示すること。また、情報管理体制図にはインシデント発生時の連絡先と連絡方法を示すこと。

受注者は、インシデント発生又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

７．利用するクラウドサービスにバックアップ機能を有していること。また、バックアップ機能を有していない場合は、協議の上で受注者または発注者がバックアップを行うこと。

８．受注者は、発注者の設定内容に変更を行う場合は、２名以上で作業しその内容を記録すること。

９．利用するクラウドサービスに不正操作の有無について確認できるログ取得機能を有していること。また、ログ管理機能を有していない場合は、受注者がログを発注者の求めに応じて随時提供すること。また、ログについては、過去２年間分保存を行うこととする。なお監査及び事実解明に必要である場合は発注者の求めに応じて取得・共有することとする。

10. 受注者は、サービス利用停止やインシデント等の発生時にはその原因追及と対応を行うとともに、発注者へ報告を行い記録すること。

11. 利用するクラウドサービスがアクセス制御機能及びログイン機能を有していること。

12. 情報システム開発業務の場合、受注者は作業者のハードおよびソフトを特定して、それ以外のものを利用させないこと。

13. 情報システムの本市ネットワーク内への導入業務の場合、開発、テスト、本番運用環境を分離し、本番環境への接続・移行を行う場合は、移行手順を明確化し、テストを実施した上で接続・移行を行うこと。

開発および保守で事業者が異なる場合や、導入システム事業者とネットワーク管理者が異なる場合などは事業者間の打合せを綿密に行い、移行に伴う情報システム停止などの影響が最小限になるよう万全を期すこと。

14. 提供するクラウドサービスが、故意または過失により情報が改ざんされる又は漏洩する恐れがある場合にこれを検出するチェック機能を有していること。

提供するクラウドサービスに、サポート期限ほかサービス提供に影響する脆弱性を検出した場合は速やかに担当職員に情報提供を行うとともに、脆弱性対策を講ずること。

15. 受注者は、不正プログラムへの対策を行い、提供するクラウドサービスが不正プログラムを含まないようにすること。

16. 提供するクラウドサービスが、不正アクセスによる改竄検出機能及びアクセス制御機能を有していること。

　受注者が発注者の管理者権限を与えられる場合、多要素認証を用いてログインを行うこと。

17. 提供するクラウドサービスが、標的型攻撃に対して、侵入防止機能や攻撃検出機能を有すること。

18. 受注者は、提供するクラウドサービスにおいてセキュリティに関する事案を検知するためシステム監視機能を備え、システム監視を行うこと。

　受注者は、発注者や利用者側で行う操作に関して、セキュリティインシデントを防ぐためにも、操作に関する手順書を提供すること。

19. 受注者は職務の遂行において使用する情報資産を保護するために、次の法令ほか関連法令を遵守すること

（１）著作権法

（２）不正アクセス行為の禁止に関する法律

（３）個人情報の保護に関する法律

（４）サイバーセキュリテイ基本法

（５）袋井市個人情報の保護に関する法律施行条例

20. 受注者は、情報セキュリティマネジメントシステム（ISO27001）またはそれと同等の第三者認証を取得していること。

21. 受注者は、発注者が情報セキュリティ要件に沿って、必要なセキュリティ対策が確保されているか受注者に情報提供を求めた場合は対応すること。また、市が必要に応じて実施する監査、検査を受け入れること。

22. 受注者は、インシデント発生時に必要に応じて発注者側から公表を行うことをあらかじめ承知すること。

23. 発注者は、受注者がセキュリティ要件の遵守をせず、再三の指示に対して対策を講じなかった場合、仕様書要件の不履行として契約解除を行うことを可能とする。

24. 別途定めるサービスレベルを遵守すること

25. 情報資産を管理するデータセンタの設置場所は、国内とすること。契約の解釈・準拠法は日本法に基づくものとし、クラウドサービスの利用契約に関連して生じる一切の紛争は、日本国内の裁判所を専属的合意管轄裁判所とすること。

別紙２

住所

名称

代表者氏名

担当者氏名

情報セキュリティ要件遵守報告書

情報セキュリティの規定に基づき、根拠資料と共に下記のとおり報告します。

契約件名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（記入方法　確認実施状況欄に「確認済」「○月実施予定」等を記載）

項目	確認事項	確認実施状況（契約前）	確認実施状況（完了時）
1	受注者は、情報セキュリティ要件をあらかじめ確認し、再委託先がある場合は再委託先も含めて、情報セキュリティ用件を遵守できることを確認した上で入札または見積書の提出を行うこと。 また、発注者が定める「情報管理体制図」及び「情報セキュリティ要件遵守報告」を、袋井市役所の本事業担当職員に契約締結前と事業終了時に根拠資料とともに担当職員に提出すること。 なお、報告の内容について、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。 加えて、事業実施期間中にこれらに変更が生じる場合は、事前に担当職員へ案を提出し同意を得ること。		
2	受注者は、本業務を再委託する場合は、再委託先においても本セキュリティ要件を遵守するよう再委託先を指導し、遵守状況の確認を行うこと。 また、本業務を再委託する場合は「情報管理体制図」には再委託先の従事者等を含めること。		
3	受注者は、本業務遂行中に得た本業務に関する情報の取扱いには十分注意を払い、漏洩を防ぐこと。 受注者は、サービスを終了または契約終了する際には、予め定めた方法によってサービス上のデータの移管及び消去を行うとともに、受注者においては本業務遂行中に得た本業務に関する情報を速やかに消去すること。 なお、サービス上のデータの移管及び消去に関して発注者側で行う場合は、受注者はその方法を提示し、確実な消去を行えるようにすること。 消去を実施した旨を、事業終了時に「情報セキュリティ要件遵守報告」に記載して提出すること。		

	受注者は、契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。		
4	受注者は、本業務で利用した機器を廃棄する場合は、予め定めた方法でデータの移管及び消去を行うとともに、機器内のデータを復元不能な状態で廃棄し、事業終了時に「情報セキュリティ要件遵守報告」に記載して提出すること。		
5	受注者は、本業務で提供するクラウドサービスおよび本業務で使用するソフトウェア、電子計算機等について、脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じること。 加えて、これらの対策を含め情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。		
6	受注者は、本業務に従事する者を限定し、従事する者の氏名、所属、専門性、国籍、連絡先をまとめた「情報管理体制図」を担当職員に提示すること。また、情報管理体制図にはインシデント発生時の連絡先と連絡方法を示すこと。 受注者は、インシデント発生又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。		
7	利用するクラウドサービスにバックアップ機能を有していること。また、バックアップ機能を有していない場合は、協議の上で受注者または発注者がバックアップを行うこと。		
8	受注者は、発注者の設定内容に変更を行う場合は、２名以上で作業しその内容を記録すること。		
9	利用するクラウドサービスに不正操作の有無について確認できるログ取得機能を有していること。また、ログ管理機能を有していない場合は、受注者がログを１カ月に１回発注者に提供すること。なお監査及び事実解明に必要である場合は発注者の求めに応じて取得・共有することとする。		
10	受注者は、サービス利用停止やインシデント等の発生時にはその原因追及と対応を行うとともに、発注者へ報告を行い記録すること。		
11	利用するクラウドサービスがアクセス制御機能及びログイン機能を有していること。		
12	情報システム開発業務の場合、受注者は作業者のハードおよびソフトを特定して、それ以外のものを利用させないこと。		
13	情報システムの本市ネットワーク内への導入業務の場合、開発、テスト、本番運用環境を分離し、本番環境への接続・移行を行う場合は、移行手順を明確化し、テストを実施した上で接続・移行を行うこと。 開発および保守で事業者が異なる場合や、導入システム事業者とネットワーク管理者が異なる場合などは事業者間の打合せを綿密に行い、移行に伴う情報システム停止などの影響が最小限になるよう万全を期すこと。		
14	提供するクラウドサービスが、故意または過失に		

	より情報が改ざんされる又は漏洩する恐れがある場合にこれを検出するチェック機能を有していること。 提供するクラウドサービスに、サポート期限ほかサービス提供に影響する脆弱性を検出した場合は速やかに担当職員に情報提供を行うとともに、脆弱性対策を講ずること。		
15	受注者は、不正プログラムへの対策を行い、提供するクラウドサービスが不正プログラムを含まないようにすること。		
16	提供するクラウドサービスが、不正アクセスによる改竄検出機能及びアクセス制御機能を有していること。 受注者が発注者の管理者権限を与えられる場合、多要素認証を用いてログインを行うこと。		
17	提供するクラウドサービスが、標的型攻撃に対して、侵入防止機能や攻撃検出機能を有すること。		
18	受注者は、提供するクラウドサービスにおいてセキュリティに関する事案を検知するためシステム監視機能を備え、システム監視を行うこと。 受注者は、発注者や利用者側で行う操作に関して、セキュリティインシデントを防ぐためにも、操作に関する手順書を提供すること。		
19	受注者は職務の遂行において使用する情報資産を保護するために、次の法令ほか関連法令を遵守すること （１）著作権法 （２）不正アクセス行為の禁止に関する法律 （３）個人情報の保護に関する法律 （４）サイバーセキュリテイ基本法 （５）袋井市個人情報の保護に関する法律施行条例		
20	受注者は、情報セキュリティマネジメントシステム（ISO27001）またはそれと同等の第三者認証を取得していること。		
21	受注者は、発注者が情報セキュリティ要件に沿って、必要なセキュリティ対策が確保されているか受注者に情報提供を求めた場合は対応すること。また、市が必要に応じて実施する監査、検査を受け入れること。		
22	受注者は、インシデント発生時に必要に応じて発注者側から公表を行うことをあらかじめ承知すること。		
23	発注者は、受注者がセキュリティ要件の遵守をせず、再三の指示に対して対策を講じなかった場合、仕様書要件の不履行として契約解除を行うことを可能とする。		
24	別途定めるサービスレベルを遵守すること		
25	情報資産を管理するデータセンタの設置場所は、国内とすること。契約の解釈・準拠法は日本法に基づくものとし、クラウドサービスの利用契約に関連して生じる一切の紛争は、日本国内の裁判所を専属的合意管轄裁判所とすること。		

別紙３

住所
名称
代表者氏名
担当者氏名

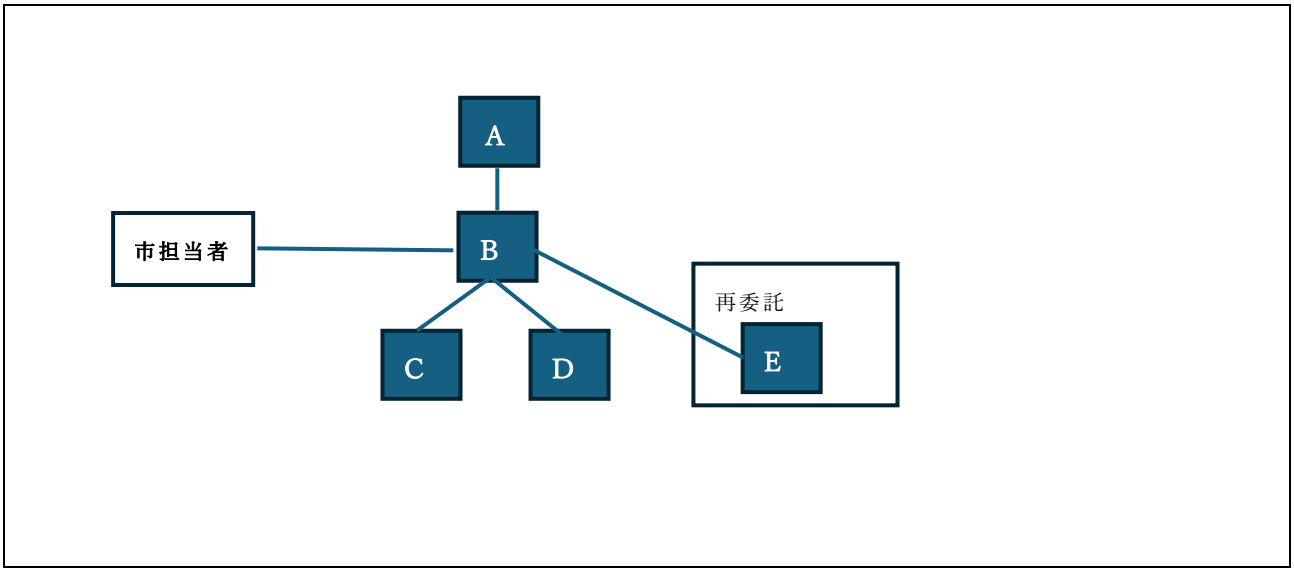
情報管理体制図

情報セキュリティの規定に基づき、情報管理と実施体制等について報告します。
契約件名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

名簿

	氏名	所属	役割	Email	連絡窓口 緊急時 電話番号	国籍	情報 管理 責任者
A							○
B					○ XXX-XXXX- XXXX		
C							
D							
E							

体制図



緊急時対応

緊急時対応	連絡方法	対応方針
システム予定停止時	（例）メンテナンス情報はBから市担当者へ事前連絡	（例）受注者側にてアプリ利用者へ情報発信（アプリ上掲載、ホームページ掲載等）を行ったうえでメンテナンスを行う。
システム停止時	（例）Bと市担当者が電話またはメールで連絡し情報共有	（例）受注者は速やかに復旧対応と原因究明を行う。〇時間以上のシステム停止を目途に以下対応を行う。 （事業者）アプリ利用者への状況配信 （市）市ホームページへの状況＆代替方法掲載
情報漏洩等インシデント発生時	（例）市担当者が電話またはメールで連絡し情報共有	（例）受注者はインシデント調査を行うとともに市担当者に状況報告を行う。