情報システムに関する業務委託契約事項

１　操作手順

情報システム等の操作手順は文書化し、最新の状態を維持すること。また、その手順は、必要とする全ての利用者に対して利用可能とすること。

２　不正プログラム対策

（１）受注者は、利用するパソコンやサーバ等に不正プログラム対策ソフトウェアの最新バージョン及び定義ファイルを維持管理し、不正プログラムを検出する措置を行うこと。不正プログラムが検知された場合は速やかに検知された不正プログラムを自動的に隔離し駆除するとともに、発注者に報告すること。またネットワークから遮断し、改ざんが確認された場合は、発注者と相談の上、正しい内容に復元すること。

（２）インターネットに接続している情報システムでは、不正な攻撃を防止するための検知機能を有すること。

３　脆弱性対策

（１）受注者は、本契約の履行に際し、開発、運用、保守の際の情報セキュリティ上問題となりうるソフトウェアを使用しないこと。

（２）受注者は、情報システムの脆弱性を突いて行われる攻撃等のリスクについて情報収集を行い、業務の重要度に応じた情報セキュリティ対策を提示し、実施すること。

（３）受注者は、システム障害を未然に防止するための措置、障害発生を早期発見するための措置及び障害発生時の拡大防止や迅速復旧のための措置について、業務の重要度に応じた対策を明示すること。

（４）ウェブアプリケーションではセキュリティを考慮した実装を行い、特にインターネットに接続する情報システムでは、「脆弱性一覧」に示す脆弱性に対応すること。

（５）業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用しないこと。

４　ネットワークセキュリティ

（１）機密性の高い情報資産をインターネットに接続しているサーバ等の公開領域に保管しないこと。また、データベースサーバ等は、ファイアウォール等でインターネットと分離されたセグメントに設置すること。

（２）受注者は、情報システムの利用中に一定の使用中断時間が経過したときには、そのセッションを遮断する機能を提供すること。

（３）受注者は、情報システムの認証方法（ＩＤ、パスワード等）を発注者に提供すること。

（４）受注者は、特定の場所又は装置からの接続を認証する手段として、自動の識別装置を必要に応じて導入すること。

（５）インターネットを利用する情報システムでは、業務の重要度に応じて、ｈｔｔｐｓ、ＶＰＮ等により暗号化を行い、通信路での盗聴及び改ざんから保護すること。また不要な通信はファイアウォール等により遮断すること。

５　情報システムのログや記録

ログオンやログアウトなどの利用者の活動状況や外部からの非定常的なアクセス等のログを記録し、発注者の求めに応じて提供や点検に協力すること。

６　時刻の同期

全ての情報システム内の時刻は、正確な時刻源と同期させること。

７　情報システム停止等

情報システムを停止する場合や運用制限が生じる場合は、事前に発注者の了承を得ること。

８　変更管理

受注者が調達・管理する情報処理設備及び情報システムの変更において、発注者に影響を及ぼすものは、事前に発注者と協議を行うこと。また、情報システムの変更が行われた際には変更履歴を発注者に明示すること。

９　データベース管理

受注者が調達・管理する情報システムにおいては、発注者に割り当てられる容量・能力の限界値を開示すること。また、発注者から要請があった場合は、資源の利用率などを明示すること。

１０　バックアップ

業務継続に支障が発生する恐れのあるデータは、定期的にバックアップをとること。その際に個人情報等の機密性の高い情報資産の保護を行うこと。また、発注者がバックアップ手順を策定する場合は情報を提供すること。

１１　アクセス制御

受注者は、情報システムのアクセス制御を適切に行うこと。また、発注者がアクセス制御等の状況を確認できるようにすること。

１２　開発及び運用

（１）開発及び運用において、運用環境とテスト環境を分離すること。運用内容を変更する際には、テスト実施及び検証結果を事前に発注者へ報告し、承認を得ること。なお、外部でテストをする際は、必要に応じて実施及び検証のテストデータに、個人情報及び一般に公表することを前提としていない情報資産の実在データが含まれないようにすること。個人情報及び一般に公表することを前提としていない情報資産の実在データを含む場合は、市役所内にテスト環境をつくる等の対策を行うこと。

（２）受注者は、情報システムの利用環境に変更が生じる場合は、あらかじめ発注者に通知し、了承を得ること。

１３　入退域管理

受注者は、運用、機器の搬出入で発注者のサーバ室等機密区域へ入退域する場合は、入退域管理簿の記入等、発注者の定めた手続に従うこと。定期的に入退域しなければならない受注者は作業従事者ごとに担当する作業内容を明記した名簿を提出すること。

１４　監視

データセンター等機密性及び完全性の高い情報資産を保管する場所では、カメラ監視や入退出管理等による不審者の監視が可能な状態にすること。

脆弱性一覧

本システムに混入しないよう対処を求める脆弱性は次のとおり。

「脆弱性名称の定義に関する参照先」
（１）ＩＰＡ『安全なウェブサイトの作り方 2021 年 3 月改訂』
（２）ＣＷＥ - Common Weakness Enumeration
（３）ＩＰＡ『ウェブ健康診断仕様』

No	脆弱性名称	
1	SQL インジェクション	
2	OS コマンド・インジェクション	
3	ディレクトリ・トラバーサル脆弱性	
4	「ログイン機能」の不備	推測可能なセッション ID
		URL 埋め込みのセッション ID の外部への漏えい
		クッキーのセキュア属性不備
		セッション ID の固定化
5	クロスサイト・スクリプティング(XSS)	
6	利用者の意図に反した実行の防止機能の不備	クロスサイト・リクエスト・フォージェリ (CSRF)
		クリックジャッキング
7	メールヘッダ・インジェクション脆弱性	
8	「アクセス制御」と「認可処理」の不備	アクセス制御
		認可処理
9	HTTP ヘッダ・インジェクション	
10	eval インジェクション	
11	競合状態の脆弱性	
12	意図しないファイル公開	
13	アップロードファイルによるサーバ側スクリプト実行	
14	秘密情報表示時のキャッシュ不停止	
15	オープンリダイレクタ脆弱性（意図しないリダイレクト）	
16	クローラへの耐性	