情報セキュリティに関する特記仕様書

1　情報セキュリティポリシー及び情報セキュリティ実施手順の順守

乙は、以下のものを順守しなければならない

(1) 本市の条例、規則

(2) 本市のセキュリティポリシー

(3) 関係法令

2　セキュリティインシデント等の緊急事態の対応

(1) 乙は、本委託業務に関し、セキュリティインシデント等の緊急事態が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに甲に対して、当該事故に関わる情報の内容、件数、事故の発生場所及び発生状況を報告し、甲の指示に従わなければならない。

(2) 乙は、セキュリティインシデント等の緊急事態が発生した場合に備え、甲及びその他の関係者との連絡、証拠保全、被害拡大の防止、復旧並びに再発防止の措置を迅速かつ適切に実施するための体制を整備しなければならない。

(3) 甲は、本委託業務に関しセキュリティインシデント等の緊急事態が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

3　提供資料の保全等

契約書8条について、乙は、次の措置を講じなければならない。

(1) 資料等の利用者、作業場所及び保管場所の限定並びにその状況の台帳等への記録

(2) 施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室での資料等の保管

(3) 業務従事者以外の者が本業務で取扱う電子データにアクセスできない環境の構築

(4) 資料等を移送する場合の、移送時の体制の明確化

(5) 資料等を電子データで保管する場合の、当該データが記録された媒体及びそのバックアップの保管状況に係る確認及び点検

(6) 次のセキュリティ対策を施したパソコンの利用

ⅰ　パスワード等の認証の仕組み

ⅱ　周辺機器のアクセス制限等のデータ持ち出し制限

(7) 甲が所有するシステムを利用する場合、当該システムにおいて、甲が指定する種類又は範囲の情報以外の情報へのアクセスの禁止

(8) 本市庁舎内で業務を行う場合、名札（氏名、会社名、所属名、役職等を記し

たもの）の着用
(9) 私用パソコン、私用外部記録媒体その他の私用物での作業の禁止
(10) 機密情報を含む電子データへの暗号化処理
(11) 業務に関係のないアプリケーションのインストールの禁止
(12) 海外のデータセンター等、日本の法令が及ばない場所に電子データを保管することの禁止（ISMAP クラウドサービスリスト掲載されているサービスを利用する場合又は甲が特に認める場合を除く）
(13) その他、委託の内容に応じて、提供資料の保全のために必要な措置
(14) 上記項目の従事者への周知

4　ウイルス対策

乙は、コンピュータウイルス対策として、以下の措置を講じなければならない。
(1) 全てのサーバ及びクライアント端末にウイルス対策ソフトウェアを導入すること。
(2) ウイルス対策ソフトウェアとして、ウイルスの検知、リアルタイム保護、検疫機能などの機能を有すること。
(3) ウイルス対策ソフトウェアは常駐させること。
(4) パターンファイルの更新については、パターンファイルが公開された時点で迅速に適用できる仕組みを用意すること。
(5) ウイルス検出時には、利用者や担当職員に迅速に通知する機能を持つと同時に、駆除・削除ができること。
(6) 毎日、曜日指定、毎週、毎月等のスケジュールを作成し、定期的にウイルスチェックを行うこと。