（別紙１別紙③）

ＳＮＳを活用した相談受付対応業務におけるセキュリティに関する運用基準

① 全般

(ｱ) 情報セキュリティに関する監査を定期的に行うこと。

年１回以上実施し、結果を報告すること。

(ｲ) 事故発生時の対応計画を定め、松山市へ提出すること。

計画は、事故発生後の「受注者側対応事項」「松山市との調整・報告」「影響の分析」「ステークホルダー等への対応」などの項目と対応フローを明確にし、松山市の承認を受けること。

② 障害・災害対策

(ｱ) 障害時等の早期復旧に備え、必要に応じて機器の冗長化を図ること。

(ｲ) 障害等で一時的にデータを消失した場合、速やかに復元できること。

(ｳ) 障害等によって指定した時間帯にサービスが停止した場合は、指定した緊急連絡先に直ちに連絡するとともに、早期の運用再開を図ること。

また、経過等については随時報告すること。

(ｴ) 障害等への対策を講じるとともに、発生時の対応計画を定め、松山市へ提出すること。

③ 不正等防止対策

(ｱ) 相談員が利用する端末やその認証機能について、ＩＤやパスワードの設定及びその他のセキュリティ対策を行うこと。

また、具体的な方法について提案で示すこと。

(ｲ) ＩＤ、パスワードは適正に管理し、第三者等による不正アクセス、窃取、改ざん、消去等に対する防止措置を講じるとともに、発生時の対応計画を定め、松山市へ提出すること。業務を終了した相談員についても同様とする。

(ｳ) ウイルス、サイバー攻撃等、外部からの脅威に対し適正な対策を講じるとともに、感染時等の対応計画を定め、松山市へ提出すること。

(ｴ) 個人情報を含むデータの流出防止措置を講じるとともに、流出時の対応計画を定め、松山市へ提出すること。

(ｵ) その他ＳＮＳを活用することによるリスクや、業務を実施する上でのリスク等についてあらかじめ防止措置を講じるとともに、それぞれのリスクに応じた発生時の対応計画を定め、松山市へ提出すること。

④ データ消去

業務委託契約終了後は、記録装置について、(1)物理的な破壊、(2)磁気的な破壊、(3)ＯＳ等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、(4)ブロック消去、(5)暗号化消去のうちいずれかの方法で行い、抹消措置の完了証明書または物理的破壊の証拠写真を提出すること。

⑤　その他

(ｱ) 日本国内法が適用される国内にサーバがあること。

(ｲ) 受注者は、業務の履行に際し、他の相談と誤って回答する等、事故の発生がないよう適正な防止対策を講じるとともに、発生時の対応計画を定め、松山市へ提出すること。

(ｳ) 業務上知り得た情報についての守秘義務を徹底し、業務終了後もその効力を継続すること。