別紙２

情報セキュリティ対応状況調査書

区分	内容	対応状況（提案者記入欄）
事業者における対策	事業者の本市情報セキュリティポリシーの遵守状況（情報の取扱制限、運搬又は送信、消去等の取扱い、業務委託と外部サービスの利用等） ※提案時は総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参照すること	
	外部サービスに本市の意図しない変更が行われるなどの不正が見つかった際の原因を究明できる体制（追跡調査、立入検査、書面による体制確認等）	
	情報セキュリティインシデント対応（迅速さ・対応可能範囲・対応時間等）	
	事業者の従事者を含めた情報セキュリティ対策の実施状況の確認（確認可能か、内容、頻度、報告方法等）	
	サービス中断時の復旧（復旧時間、復旧時点、対応内容等）	
	脆弱性診断やペネトレーションテスト等の実施状況	
	クラウドサービス関連の認証の取得状況（ISO/IEC 27017やISMAP等）	
導入・構築時の対策	インターネットから利用する際の不正利用防止対策（多要素認証方式、特に管理者権限に対する制御等）	
	ログイン強度（パスワードの制限桁数・制限文字種数、過去に利用したパスワードの利用不可設定、パスワードを一定回数連続で間違えた際のアカウントロック機能等）	
	仮想マシン（本市環境）を設定・構築する際の不正プログラム対策（必要なポート、プロトコル及びサービスのみを有効とすること、マルウェア対策、ログ取得等の実施）	
	設定誤り防止（設定内容のレビュー、設定追加時の説明、設定権限をもつユーザの限定、設定誤りによるリスクの有無等）	
運用・保守時の対策	脆弱性対応（事業者・市の実施する範囲の明確化、迅速性・報告等）	
	アクセスログ（保存期間、内容、提供方法、職員による出力機能を有しているか、職員による点検が可能なログの見やすさか、ログの定期点検が可能か等）	
	管理者権限の操作記録（管理者権限の悪用を考慮した対策等）	
	不正利用の監視（不正アクセス対策、大量データダウンロード時のアラート等）	
	バックアップからの復旧（スムーズな復旧が可能か、定期的な訓練が可能か等）	