新 IΒ Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。) Ⅲ 特定個人情報の取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。) [ ]委託しない 4. 特定個人情報ファイルの取扱いの委託 [ ]委託しない 4. 特定個人情報ファイルの取扱いの委託 委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク 再委託に関するリスク 委託業者の選定に際しては、本市の入札参加資格者名簿に登載されていることを確認すると 委託業者の選定に際しては、本市の入札参加資格者名簿に登載されていることを確認するとと 情報保護管理体制の確 情報保護管理体制の確 ともに、プライバシーマーク・ISMS(情報セキュリティマネジメントシステム)の認証取得情 もに、プライバシーマーク・ISMS(情報セキュリティマネジメントシステム)の認証取得情報を 報を確認している。 確認している。 [1) 制限している 特定個人情報ファイルの [1) 制限している ] 〈選択肢〉 特定個人情報ファイルの <選択肢> 閲覧者・更新者の制限 閲覧者・更新者の制限 2) 制限していない 2) 制限していない 1) 制限している 1) 制限している 閲覧・更新権限を持つ者を必要最小限にする。 閲覧・更新権限を持つ者を必要最小限にする。 具体的な 具体的な 閲覧・更新権限を持つ者のアカウント管理を行い、システム上での操作を制限する。 閲覧・更新権限を持つ者のアカウント管理を行い、システム上での操作を制限する。 制限方法 制限方法 閲覧・更新の履歴を取得し、不正な使用がないことを確認する。 閲覧・更新の履歴を取得し、不正な使用がないことを確認する。 特定個人情報ファイルの 「1) 記録を残している ○ <選択肢> 特定個人情報ファイルの [1] 記録を残している ] **<選択肢>** 取扱いの記録 取扱いの記録 1) 記録を残している 2) 記録を残していない 1) 記録を残している 2) 記録を残していない 委託業者についても、操作履歴を記録している。 委託業者についても、操作履歴を記録している。 具体的な方法 具体的な方法 「1) 定めている ] 〈選択肢〉 「1) 定めている ] 〈選択肢〉 特定個人情報の提供ル 特定個人情報の提供ル ール 1) 定めている 2) 定めていない ール 1) 定めている 2) 定めていない 委託契約書において、第三者に提供することを禁止している。 委託契約書において、第三者に提供することを禁止している。 委託先から他者への 委託先から他者への 委託契約書の条項に違反する事態が生じるおそれがあるが場合は、速やかに報告書を提出さ 委託契約書の条項に違反する事態が生じるおそれがあるが場合は、速やかに報告書を提出させ 提供に関するルール 提供に関するルール せる。 の内容及びルール導 の内容及びルール導 守の確認方法 守の確認方法 委託元と委託先間の 委託している業務については、本市庁舎内に設置されたシステムを使用して作業を実施しているため、特定 委託契約書において、提供した原始資料等の管理について明記している。 委託元と委託先間の 委託契約書の条項に違反する事態が生じるおそれがあるが場合は、速やかに報告書を提出させる。 提供に関するルール 提供に関するルール 個人情報を委託先には提供していない。 の内容及びルール遵 の内容及びルール遵 守の確認方法 守の確認方法 <選択肢> <選択肢> [1) 定めている [1) 定めている 特定個人情報の消去ル 特定個人情報の消去ル ール 1) 定めている 2) 定めていない ール 1) 定めている 2) 定めていない 委託契約書において、提供した原始資料等の返還及び処分について明記している。 委託業者に特定個人情報を提供していないため、データの消去の委託はしていない。 ルールの内容及びル ルールの内容及びル 委託契約書の条項に違反する事態が生じるおそれがあるが場合は、速やかに報告書を提出させる。 ール遵守の確認方法 ール遵守の確認方法 [1) 定めている ] 〈選択肢〉 [1) 定めている ] 〈選択肢〉 委託契約書中の特定個 委託契約書中の特定個 人情報ファイルの取扱いに 1) 定めている 2) 定めていない 人情報ファイルの取扱いに 2) 定めていない 1) 定めている 関する規定 関する規定 目的外利用の禁止 目的外利用の禁止 ・情報漏えい等を防ぐための適正管理 ・情報漏えい等を防ぐための適正管理 ・ 複写等の禁止 複写等の禁止 規定の内容 規定の内容 ・再委託の禁止 再委託の禁止 · 事故報告義務 · 事故報告義務 [4] 再委託していない <選択肢> [4) 再委託していない ] <選択肢> 再委託先による特定個人 再委託先による特定個人 1) 特に力を入れて行っている 2) 十分に行っている 1) 特に力を入れて行っている 2) 十分に行っている 情報ファイルの適切な取扱 情報ファイルの適切な取扱 いの確保 いの確保 3) 十分に行っていない 4) 再委託していない 3) 十分に行っていない 4) 再委託していない 具体的な方法 具体的な方法 その他の措置の内容 その他の措置の内容 [2) 十分である] く選択肢> [2) 十分である] く選択肢> 1) 特に力を入れている 2) 十分である リスクへの対策は十分か 1) 特に力を入れている 2) 十分である リスクへの対策は十分か 3) 課題が残されている 3) 課題が残されている 特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置 特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置