## 予防接種に関する事務の特定個人情報保護評価書（全項目評価書）（素案）への意見募集の結果について

２０２１年（令和３年）９月１日から１０月１日までの間に実施した「明石市 予防接種に関する事務 全項目評価書（案）」に関する意見募集の結果は、下記のとおりです。

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 1 | 11 | Ⅱ　特定個人情報ファイルの概要<br>４　特定個人情報ファイルの取扱いの委託<br>委託事項１<br>⑤委託先への特定個人情報ファイルへの提供方法<br><br>（記載内容）<br>［〇］その他<br>本市事務室において、直接端末操作を行う | ・明確に、「委託先へ特定個人情報ファイルを提供することはない（作業は本市事務室内の端末を利用）」したほうが分かりやすい。（左記の記載は同趣旨かもしれませんが。）<br>・「①委託内容」から想定すると、「本市事務室」には、サーバー設置場所や情報システム室内を含んでいるように思われます。そうであれば、一般事務室と誤解されないような記載にした方が分かりやすい。<br>１２頁の「委託事項２」の④も同様。 | 保守作業において個人番号を確認することがあるため、委託先への特定個人情報の閲覧はあるものと考えます。なお、特定個人情報ファイルそのものを提供することはありません。<br>また、作業時は、業務担当課の課室、サーバー室に設置している端末を利用します。いずれも専用のネットワーク上で運用しているため、その旨での記載といたします。 |
| 2 | 11 | Ⅱ　特定個人情報ファイルの概要<br>４　特定個人情報ファイルの取扱いの委託<br>委託事項１<br>⑧再委託の許諾方法 | 「本市承諾」にあたって、「承諾書」の交付があれば、その旨を追記してはどうでしょうか。（承諾書交付の手続がなければ、今後検討されてはどうでしょうか。）<br>１２頁の「委託事項２」の⑧も同様。 | 再委託の承諾は、承諾書の交付により実施しております。その旨について、追記いたします。 |
| 3 | 13 | Ⅱ　特定個人情報ファイルの概要<br>４　特定個人情報ファイルの取扱いの委託<br>委託事項３<br>⑤委託先名の確認方法 | 前記「特定個人情報保護評価書（全項目評価書）【記載要領】」によれば、「委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を記載してください。」とあり、左記の記載では不十分であるように思われます。<br>「委託事項１」の⑤や「委託事項２」の⑤の記載と同様とすることで問題ないのではないでしょうか。 | 本委託契約は、本市が実施したものではなく、国がまとめて契約したものです。そのため、本市に開示請求をいただいても、委託先について開示できる資料はありません。<br>なお、本保護評価の記載は、国が「特定個人情報保護評価指針」に基づき、各市町村に情報提供をした内容を記載しております。 |

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 4 | － | Ⅱ　特定個人情報ファイルの概要<br>４　特定個人情報ファイルの取扱いの委託 | １６頁の「６．特定個人情報の保管・消去」の「①保管場所」において、「バックアップデータを遠隔地に保管している。（保健情報管理システムＴＩＡＲＡ及び共通宛名システムのみ）」とされています。この場合、「バックアップ媒体の運搬」や「バックアップ媒体の保管」に関する業務委託は発生していないのでしょうか。当該業務委託があれば、追記されることが望まれます。 | システムのバックアップについては、保管と集配を合わせて業務委託をしております。その旨について追記いたします。 |
| 5 | 20 | Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>３．特定個人情報の使用<br>リスク２<br>ユーザー認証の管理 | パスワードを定期的及び随時変更するような周知活動の有無や、システム的に変更を求める設定となっていないのでしょうか。該当あれば、追記されることが望まれます。 | パスワードの変更について、研修において周知するとともに、システム上でも変更するように設定をしています。研修については「Ⅳ　その他のリスク対策　２．従業者に対する教育・啓発」にて記載している内容と同一になるため、システムに関する内容のみ追記します。 |

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 6 | ― | Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>３．特定個人情報の使用<br>リスク２<br>ユーザー認証の管理 | 前記「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」の「第３編」の「第２章　情報セキュリティ対策基準（解説）５．４．ＩＤ及びパスワード等の管理」によれば、パスワードの取扱いを下記のとおりとされています。当該事務において、適用されている事項について、追記されてはどうでしょうか。<br>（３）パスワードの取扱い<br>職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。<br>①パスワードは、他者に知られないように管理しなければならない。<br>②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。<br>③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。<br>④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。<br>⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。<br>⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。<br>⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。<br>⑧職員等間でパスワードを共有してはならない（ただし、共有ＩＤに対するパスワードは除く）。 | 「地方公共団体における情報セキュリティポリシーの関するガイドライン」等に基づき、「明石市情報セキュリティ基本方針」「明石市情報セキュリティ対策基準」を定めております。本方針および基準に基づき、パスワードについても管理しているため、個別に記載は行いません。 |

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 7 | 20 | Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>３．特定個人情報の使用<br>リスク２<br>アクセス権限の発効・失効の管理<br>具体的な管理方法 | 前記「特定個人情報保護評価書（全項目評価書）【記載要領】」によれば、下記のとおりとあり、「発行管理」及び「失効管理」それぞれについて、分けて記載する方が分かりやすい。<br>「・特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報（ユーザＩＤ、パスワード等）の発効・失効の管理を行う場合は、以下の点について記載してください。<br>（１）発効管理：事務上必要なユーザについてのみＩＤ等を発効するようにどのような手段を講じているか（権限発効のポリシー、申請・許可の流れ等を記載してください）。更新権限者を不必要に増やさないためにどのような手段を講じているか。<br>（２）失効管理：事務範囲の変更、異動、休職、退職など、事務上情報にアクセスする必要のなくなったユーザの権限を迅速に失効するためにどのような手段を講じているか（たとえば、権限失効の流れを記載してください）。<br>・発効・失効の管理を行わない場合、行わなくても権限のない者による不正な使用を防止できる理由を記載してください。 | 人事異動時に作成する書類は、「発行管理」および「失効管理」を合わせて実施する様式としています。分かりにくい表現であったため、追記いたします。 |
| 8 | 20 | Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>３．特定個人情報の使用<br>リスク２<br>アクセス権限の発効・失効の管理<br>具体的な管理方法 | 左記に加えて、ユーザーＩＤやアクセス権について、事務担当部署や情報システム部署の管理者が定期的に確認し、その妥当性を検証し、アクセス権限の見直しにつなげるなどの対応を行っていないのでしょうか。<br>あれば、追記されることが望まれます。 | 権限の変更は、業務内容の追加・変更のタイミングで見直しをしています。なお、システム利用の必要性を含め、権限の見直しは、年に１度実施しています。 |

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 9 | 22 | Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>４．特定個人情報ファイルの取扱いの委託<br>情報保護管理体制<br>の確認 | 情報保護管理体制の確認については、①業者選定時、②契約時、③契約締結後（運用段階）の３段階に分けて考えることができます。<br>左記記載は、主に業者選定時の確認事項と考えられます。<br>再委託先を含め、委託先との契約時において、委託先の個人情報保護に関する規定や体制の整備、個人情報保護に関する安全管理措置などの確認が必要ではないでしょうか。<br>また、契約締結後において、必要に応じて実地の監査、調査等を行う等、契約締結後に情報保護管理体制の確認を行うことなどを契約書に盛り込む必要はないでしょうか。<br>ただし、２２頁の「委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法」において、下記のとおりとされているため、対応されているとも理解される。<br>＜システム運用・保守について＞<br>・業務委託に関しては、委託契約にて委託業務実施場所を本市事務所内に限定している。<br>・委託契約の調査報告条項に基づき、必要があると認めるときは調査を行い、または報告を求める。 | ①業者選定時、②契約時、③契約締結後のそれぞれについて、情報保護管理体制を確認する必要があることは認識しており、確認もしております。契約時には、２２頁「特定個人情報ファイルの閲覧者・更新者の制限」に記載しておりますように、実施体制の報告を求めています。また、契約締結後については、ご指摘の箇所に記載しておりますように、管理体制等について報告を求めています。 |
| 10 | 22 | Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策<br>４．特定個人情報ファイルの取扱いの委託<br>委託契約書中の特定個人情報ファイルの取扱いに関する規定<br>規定の内容 | １１頁の「委託事項１」の「⑧再委託の許諾方法」において、「・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。」とされていますが、このことについて、再（もしくは再々）委託先について、契約書上の取り決めは、特に用意されていないのでしょうか。<br>この件について、契約書に明記されていなければ、今後検討されてはどうでしょうか。 | 再委託先についても、個人情報保護の措置を実施するよう契約書上に規定し、その措置は本市が委託先に対して課している措置と同様のものであることを求めています。本評価書２３ページ「再委託先による特定個人情報ファイルの適切な取扱いの確保－具体的な方法」に記載の通りです。 |

| No. | 頁 | 記載箇所 | 意見 | 回答 |
|---|---|---|---|---|
| 11 | 30 | Ⅳ その他のリスク対策<br>１．監査<br>②監査<br>具体的な内容 | 監査の実施の詳細については、「明石市情報セキュリティ基本方針」及び「明石市特定個人情報等取扱基準」に記載されていると思われるが、当該本文においても、３０頁「①自己点検」と同様に、どの部署が実施するのか、頻度はどれくらいかについて記載されることが望ましい。その場合、監査の独立性、客観性、監査人の専門性が担保されていることに留意されることが望ましい。 | 内部監査につきましては、年に１回、２～３課を対象として実施しています。監査を実施するのは、前年度の監査対象課及び情報管理課です。監査においては、自己点検結果に基づき、運用状況を改めて確認しています。 |
| 12 | 30 | Ⅳ その他のリスク対策<br>１．監査<br>②監査 | 前記「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」の「第２章 情報セキュリティ対策基準（解説）９評価・見直し９．１．監査」において、下記のとおりとされており、再委託先を含む外部委託業者に対する監査も検討する必要があるのではないでしょうか。<br>（例文）<br>（４）外部委託事業者に対する監査<br>外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。<br>（解説）<br>（４）外部委託事業者に対する監査<br>情報システムの運用、保守等を外部委託している場合は、情報資産の管理が契約に従い適正に実施されているかを点検、評価する必要がある。また、これによって、セキュリティ侵害行為に対する抑止効果も期待できる。 | 現時点では、先に回答いたしましたとおり、契約履行期間中の実施体制の報告により、適切な管理がされているかを確認しています。 |