# 特定個人情報保護評価書（全項目評価書）

| 評価書番号 | 評価書名 |
| --- | --- |
| 6 | 国民年金に関する事務　全項目評価書 |

## 個人のプライバシー等の権利利益の保護の宣言

堺市は、国民年金事務における特定個人情報ファイルの取り扱いについて、特定個人情報の漏えいやその他の事態発生による個人のプライバシー等の権利利益に与える影響を認識し、このようなリスクを軽減するための適切な措置を講じたうえで、個人のプライバシー等の権利利益の保護を実施していることを宣言する。

| 特記事項 | 国民年金事務では、事務の一部を外部業者に委託しているため、業者選定の際に業者の情報の保護管理体制を確認し、併せて秘密保持に関しても契約に含めることで万全を期している。 |
| --- | --- |

## 評価実施機関名

大阪府堺市長

## 個人情報保護委員会　承認日 【行政機関等のみ】

## 公表日

［平成30年５月　様式４］

# 項目一覧

# Ⅰ　基本情報

| 1．特定個人情報ファイルを取り扱う事務 | |
|---|---|
| ①事務の名称 | 国民年金に関する事務 |
| ②事務の内容　※ | 本市では、「国民年金法」（以下「国年法」という。）及び「行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年5月31日法律第27号）」（以下「番号法」という。）に基づき、特定個人情報を以下の国民年金事務で取り扱う。（別添1を参照）<br><br>1．届出・申出<br>①第1号被保険者及び任意加入被保険者の適用に関する事務<br>・資格取得及び喪失、種別変更、死亡、氏名及び住所変更に関する届出等の受理並びに受付記録の作成<br>・資格記録、生年月日、性別訂正に関する受付記録の作成<br>・手帳（R4.4.1～基礎年金番号通知書）再交付申請の受理並びに受付記録の作成<br><br>②付加保険料に関する事務<br>・付加保険料の納付または納付しないことの申出の受理並びに受付記録の作成<br><br>③法定免除に関する事務<br>・法定免除の該当または不該当届出受理並びに受付記録の作成<br><br>2．申請<br>④保険料免除・納付猶予に関する事務<br>・国民年金保険料免除、納付猶予、学生納付特例の申請受付並びに受付記録の作成<br><br>3．請求・届出<br>⑤老齢基礎年金ほか年金及び一時金の請求手続き・受給権者からの届出に関する事務<br>・老齢基礎年金、障害基礎年金、遺族基礎年金、寡婦年金、死亡一時金等に関する請求受付並びに受付記録の作成<br>・受給権者からの届出又は申出の受理並びに受付記録の作成<br><br>4．報告<br>⑥厚生労働大臣（日本年金機構）への報告<br>・受理した届出書等を日本年金機構へ送付する<br><br>5．処理結果管理<br>⑦日本年金機構から送付された処理結果管理<br>・日本年金機構から送付される処理結果一覧に基づき、被保険者及び受給者情報を登録する |
| ③対象人数 | [　30万人以上　] ＜選択肢＞<br>1）1,000人未満　2）1,000人以上1万人未満<br>3）1万人以上10万人未満　4）10万人以上30万人未満<br>5）30万人以上 |

| 2. 特定個人情報ファイルを取り扱う事務において使用するシステム | |
|---|---|
| **システム1** | |
| ①システムの名称 | 国民年金システム |
| ②システムの機能 | 1. 情報照会機能<br>被保険者及び受給者に関する情報照会を行う。<br><br>2. 情報更新機能<br>被保険者及び受給者に関する情報の作成または修正を行う。<br><br>3. 国民年金保険料免除等に関する入力機能<br>国民年金保険料の免除等の申請受付、免除判定試算、免除等審査結果の入力管理を行う。<br><br>4. 届書等の発行機能<br>国民年金関係届書や免除等申請書などを発行する。<br><br>5. 日本年金機構への送付帳票作成機能<br>受理した届書等の情報を一覧にして出力する。<br><br>6. 統計情報作成機能<br>異動情報等の集計表を作成する。<br><br>7. 年金情報削除機能<br>被保険者及び受給権者情報を削除する。 |
| ③他のシステムとの接続 | [　] 情報提供ネットワークシステム　[　] 庁内連携システム<br>[　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム<br>[　] 宛名システム等　[　] 税務システム<br>[ ○ ] その他　（ 保険年金共通システム　） |
| **システム2** | |
| ①システムの名称 | 共通基盤システム |
| ②システムの機能 | 1. データ連携機能<br>:住民情報系システム間で、定例に提供、利用しているデータ(住民の転出入データ等)を連携する機能。<br><br>2. ウイルス対策機能<br>:住民情報系システム全体のウイルス対策ソフトを統括し、ウイルス定義ファイルの配信を行う機能。<br><br>3. ディレクトリサービス機能(Active Directory)<br>:システムを利用できるユーザや組織、コンピュータ等の情報とその属性を階層的に管理し、認証機能を提供する。<br><br>4. 更新プログラム配布機能(Windows Server Update Services(WSUS))<br>:脆弱性等に対応する更新プログラムを配布、管理する機能。<br><br>5. 文字管理機能<br>:文字変換及び外字一元管理、外字配布を行う機能。<br><br>6. 帳票出力機能<br>:共通基盤印刷専用ソフトウェア(Interstage List Creator)により印刷を行う機能。<br><br>7. 持ち出し制限機能<br>:使用できる媒体を制限するとともに端末からデータを持ち出す際は上長の承認を必須とする機能。<br><br>8. 生体認証機能<br>:Windowsログイン認証前に生体(顔)による認証を行う機能。 |
| ③他のシステムとの接続 | [　] 情報提供ネットワークシステム　[ ○ ] 庁内連携システム<br>[　] 住民基本台帳ネットワークシステム　[ ○ ] 既存住民基本台帳システム<br>[ ○ ] 宛名システム等　[ ○ ] 税務システム<br>[ ○ ] その他　（ 連携するシステムすべて　） |

| システム3 | |
|---|---|
| ①システムの名称 | 保険年金共通システム |
| ②システムの機能 | 1　国民年金システム、国民健康保険システム、障害者医療費助成システム、老人医療費助成システム、<br>　ひとり親家庭医療費助成システム及び子ども医療費助成システム（以下、保険年金システムという。）の利用者及びアクセス権限を管理する機能<br>2　共通基盤システムから連携した住基・税情報等を蓄積し、保険年金システムから参照させる機能<br>3　他システムへ提供する情報を共通基盤システムへ連携する機能<br>4　システムに接続（アクセス）するパソコン、プリンタ等の機器を管理する機能<br>5　金融機関等の各種マスタを管理する機能 |
| ③他のシステムとの接続 | ［ ○ ］情報提供ネットワークシステム　　［ ○ ］庁内連携システム<br>［　　］住民基本台帳ネットワークシステム　　［　　］既存住民基本台帳システム<br>［ ○ ］宛名システム等　　［　　］税務システム<br>［ ○ ］その他　（ 保険年金システム　　） |

| システム4 | |
|---|---|
| ①システムの名称 | 国民年金システム　※標準準拠システム移行後 |
| ②システムの機能 | 1. 情報照会機能<br>被保険者及び受給者に関する情報照会を行う。<br><br>2. 情報更新機能<br>被保険者及び受給者に関する情報の作成または修正を行う。<br><br>3. 国民年金保険料免除等に関する入力機能<br>国民年金保険料の免除等の申請受付、免除判定試算、免除等審査結果の入力管理を行う。<br><br>4. 届書等の発行機能<br>国民年金関係届書や免除等申請書などを発行する。<br><br>5. 日本年金機構への送付帳票作成機能<br>受理した届書等の情報を一覧にして出力する。<br><br>6. 統計情報作成機能<br>異動情報等の集計表を作成する。<br><br>7. 年金情報削除機能<br>被保険者及び受給権者情報を削除する。 |
| ③他のシステムとの接続 | ［　　］情報提供ネットワークシステム　　［ ○ ］庁内連携システム<br>［　　］住民基本台帳ネットワークシステム　　［ ○ ］既存住民基本台帳システム<br>［　　］宛名システム等　　［ ○ ］税務システム<br>［ ○ ］その他　（ 共通基盤システム　　） |

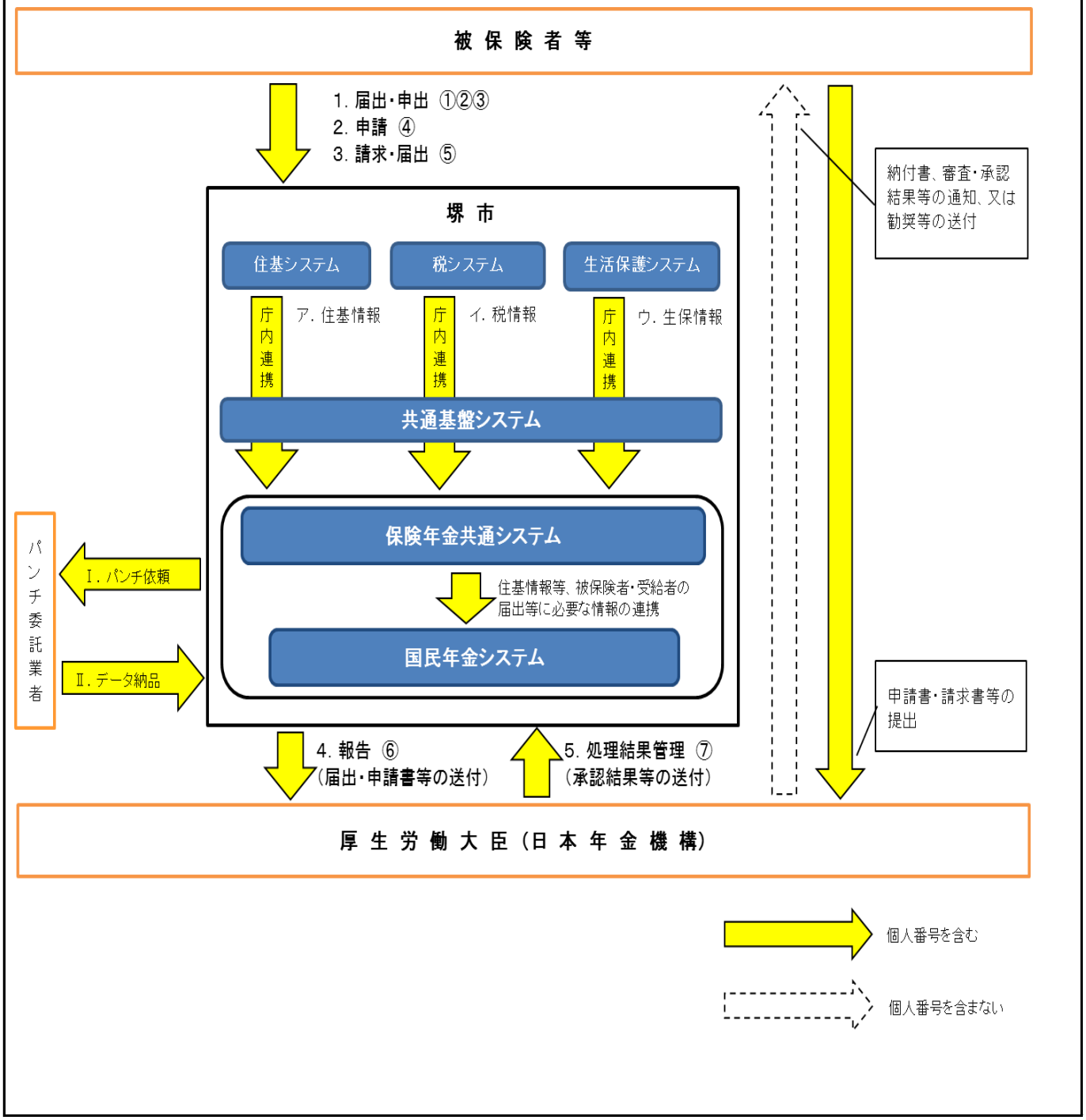
| 3. 特定個人情報ファイル名 |
|---|
| 年金情報ファイル |

| 4. 特定個人情報ファイルを取り扱う理由 | |
|---|---|
| ①事務実施上の必要性 | 国民年金被保険者又は受給権者からの資格異動届、免除等申請、年金請求を受理する上で、対象者にかかる住民情報や、所得情報を把握する必要がある。 |
| ②実現が期待されるメリット | 国民年金事務において、対象被保険者の届出や申請、年金請求時に必要となる住民情報や所得情報を、日本年金機構が直接、情報提供ネットワークを介して参照することができるため、事務処理の簡素化・効率化が図れる。 |

| 5. 個人番号の利用　※ | |
|---|---|
| 法令上の根拠 | ・番号法第九条第1項　別表第一の三十一の項<br>・行政手続における特定の個人を識別するための番号の利用等に関する法律別表第一の主務省令で定める事務を定める命令　第二十四条の二 |

| | | |
|---|---|---|
| **6. 情報提供ネットワークシステムによる情報連携 ※** | | |
| ①実施の有無 | [　　実施しない　　] | <選択肢><br>1) 実施する<br>2) 実施しない<br>3) 未定 |
| ②法令上の根拠 | | |
| **7. 評価実施機関における担当部署** | | |
| ①部署 | 健康福祉局　長寿社会部　医療年金課 | |
| ②所属長の役職名 | 医療年金課長 | |
| **8. 他の評価実施機関** | | |
| | | |

## （別添1）事務の内容


被保険者等
1. 届出・申出 ①②③
2. 申請 ④
3. 請求・届出 ⑤
堺市
住基システム
税システム
生活保護システム
庁内連携
ア. 住基情報
庁内連携
イ. 税情報
庁内連携
ウ. 生保情報
共通基盤システム
保険年金共通システム
住基情報等、被保険者・受給者の届出等に必要な情報の連携
国民年金システム
パンチ委託業者
Ⅰ. パンチ依頼
Ⅱ. データ納品
納付書、審査・承認結果等の通知、又は勧奨等の送付
申請書・請求書等の提出
4. 報告 ⑥
（届出・申請書等の送付）
5. 処理結果管理 ⑦
（承認結果等の送付）
厚生労働大臣（日本年金機構）
個人番号を含む
個人番号を含まない

（備考）

1．届出・申出
①第1号被保険者及び任意加入被保険者の適用に関する事務
②付加保険料に関する事務
③法定免除に関する事務
【処理内容】
・被保険者の住基情報及び年金情報を確認し、届出書等を受理する。
・届出内容に基づき、国民年金システムへ情報登録する。
・申請情報と登録内容に相違がないか、照合する。

2．申請
④保険料免除・納付猶予に関する事務
【処理内容】
・被保険者の年金情報及び住基情報並びに所得情報を確認し、申請書を受理する。
・申請内容に基づき、国民年金システムへ情報を登録する。
・申請情報と登録内容に相違がないか、照合する。

3．請求・届出
⑤老齢基礎年金ほか年金及び一時金の請求手続き・受給権者からの届出に関する事務
【処理内容】
・請求者等の住基情報及び年金情報を確認し、請求書又は届出書を受理する。
・請求・届出内容に基づき、国民年金システムへ情報を登録する。
・請求・届出内容と登録内容に相違がないか、照合する。

4．報告
⑥厚生労働大臣（日本年金機構）への報告
【処理内容】
・被保険者等から受理した申請書並びに請求書等について、日本年金機構へ送付する。
・被保険者等からの申請及び請求に基づいて登録した情報並びに所得情報等を、システム出力し、日本年金機構へ送付する。

5．処理結果管理
⑦日本年金機構から送付された処理結果管理
【処理内容】
・処理結果一覧表に基づいて、国民年金システムに被保険者等の情報を登録する。
・処理結果一覧表に記載の内容と登録内容に相違がないか、照合する。

ア．住基情報
堺市の住基システムから、住民登録情報を取込む（届出等の内容確認に必要）。

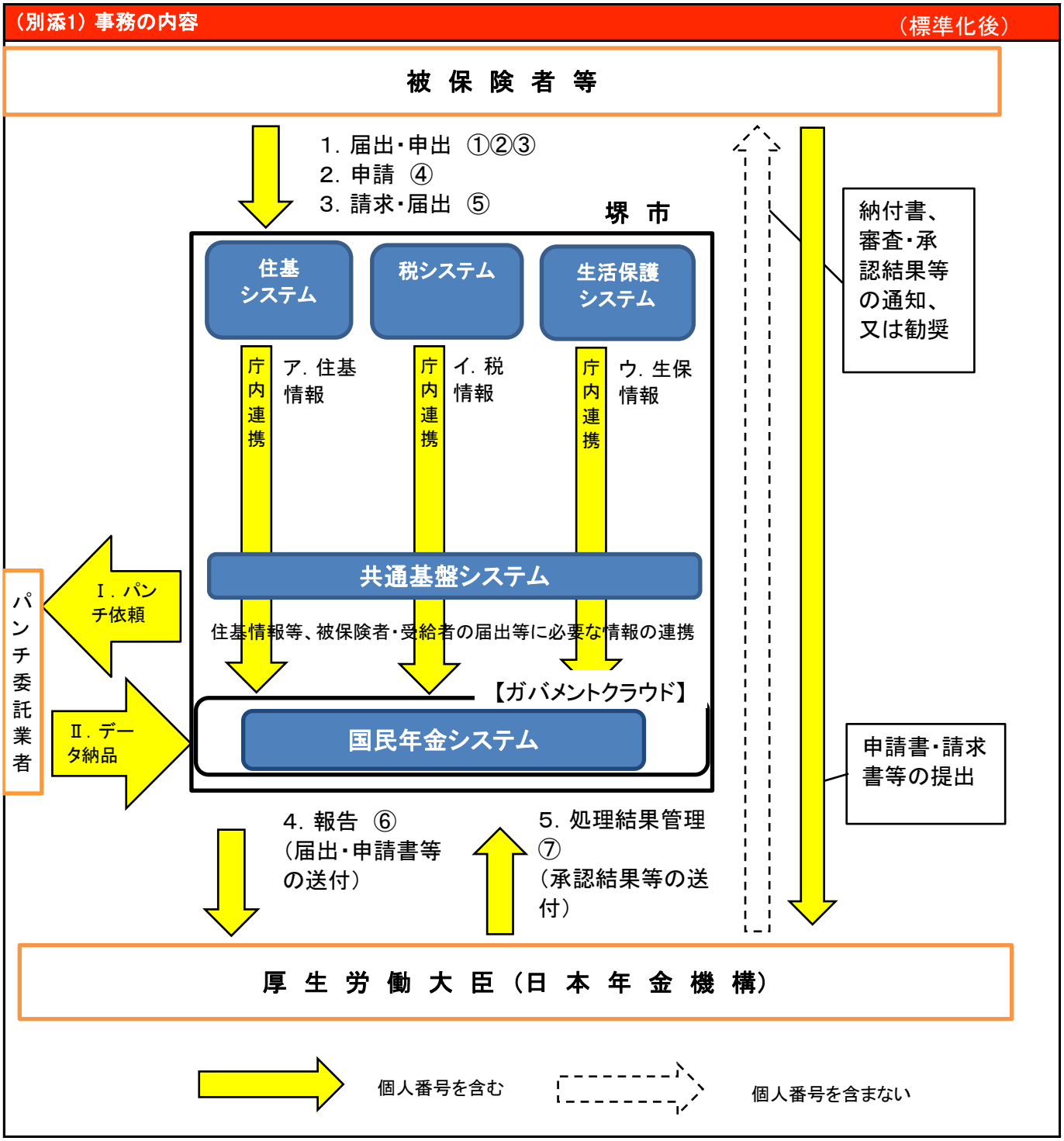
イ．税情報
堺市の税システムから、住民の税情報を取込む（免除等申請受付時に必要）。

ウ．生保情報
堺市の生活保護システムから、生活保護情報を取込む（法定免除情報の確認に必要）。

Ⅰ．パンチ依頼
日本年金機構から送付される被保険者等の処理結果一覧を、電子化するため引渡す。

Ⅱ．データ納品
引渡した処理結果一覧の返却及び電子媒体を受領し、国民年金システムに取込む。

（別添1）事務の内容　　（標準化後）



（備考）

1．届出・申出
①第1号被保険者及び任意加入被保険者の適用に関する事務
②付加保険料に関する事務
③法定免除に関する事務
【処理内容】
・被保険者の住基情報及び年金情報を確認し、届出書等を受理する。
・届出内容に基づき、国民年金システムへ情報登録する。
・申請情報と登録内容に相違がないか、照合する。

2．申請
④保険料免除・納付猶予に関する事務
【処理内容】
・被保険者の年金情報及び住基情報並びに所得情報を確認し、申請書を受理する。
・申請内容に基づき、国民年金システムへ情報を登録する。
・申請情報と登録内容に相違がないか、照合する。

3．請求・届出
⑤老齢基礎年金ほか年金及び一時金の請求手続き・受給権者からの届出に関する事務
【処理内容】
・請求者等の住基情報及び年金情報を確認し、請求書又は届出書を受理する。
・請求・届出内容に基づき、国民年金システムへ情報を登録する。
・請求・届出内容と登録内容に相違がないか、照合する。

4．報告
⑥厚生労働大臣（日本年金機構）への報告
【処理内容】
・被保険者等から受理した申請書並びに請求書等について、日本年金機構へ送付する。
・被保険者等からの申請及び請求に基づいて登録した情報並びに所得情報等を、システム出力し、日本年金機構へ送付する。

5．処理結果管理
⑦日本年金機構から送付された処理結果管理
【処理内容】
・処理結果一覧表に基づいて、国民年金システムに被保険者等の情報を登録する。
・処理結果一覧表に記載の内容と登録内容に相違がないか、照合する。

ア．住基情報
堺市の住基システムから、住民登録情報を取込む（届出等の内容確認に必要）。

イ．税情報
堺市の税システムから、住民の税情報を取込む（免除等申請受付時に必要）。

ウ．生保情報
堺市の生活保護システムから、生活保護情報を取込む（法定免除情報の確認に必要）。

Ⅰ．パンチ依頼
日本年金機構から送付される被保険者等の処理結果一覧を、電子化するため引渡す。

Ⅱ．データ納品
引渡した処理結果一覧の返却及び電子媒体を受領し、国民年金システムに取込む。

# Ⅱ　特定個人情報ファイルの概要

| 1. 特定個人情報ファイル名 | | |
|---|---|---|
| 年金情報ファイル | | |
| **2. 基本情報** | | |
| ①ファイルの種類　※ | | [　　システム用ファイル　　] ＜選択肢＞<br>1）システム用ファイル<br>2）その他の電子ファイル（表計算ファイル等） |
| ②対象となる本人の数 | | [　10万人以上100万人未満　] ＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| ③対象となる本人の範囲　※ | | ・本市に住民登録のある国民年金被保険者及びその配偶者及び世帯主<br>・本市に住民登録のある基礎年金受給者及びその世帯員<br>（本市に住民登録のあった過去の被保険者及び基礎年金受給者を含む） |
| | その必要性 | 被保険者資格取得・喪失手続き、保険料免除申請手続き、年金請求受付等の国民年金関係事務を行う上で、被保険者等に関する世帯情報・所得情報等を把握する必要がある。 |
| ④記録される項目 | | [　　100項目以上　　] ＜選択肢＞<br>1）10項目未満　2）10項目以上50項目未満<br>3）50項目以上100項目未満　4）100項目以上 |
| | 主な記録項目　※ | ・識別情報<br>[ ○ ] 個人番号　[　] 個人番号対応符号　[ ○ ] その他識別情報（内部番号）<br>・連絡先等情報<br>[ ○ ] 4情報（氏名、性別、生年月日、住所）　[ ○ ] 連絡先（電話番号等）<br>[ ○ ] その他住民票関係情報<br>・業務関係情報<br>[　] 国税関係情報　[ ○ ] 地方税関係情報　[　] 健康・医療関係情報<br>[　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報<br>[ ○ ] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報<br>[　] 雇用・労働関係情報　[ ○ ] 年金関係情報　[　] 学校・教育関係情報<br>[　] 災害関係情報<br>[　] その他　（　　） |
| | その妥当性 | 『個人番号』『その他識別情報』：　対象者を正確に特定するために必要<br>『4情報』『連絡先』：　国民年金加入・喪失届出時の住所確認、転出・死亡による異動処理、本人への連絡等のため必要<br>『その他住民票関係情報』『地方税関係情報』『生活保護・社会福祉関係情報』：　保険料免除等申請にかかる審査、年金請求時における審査を行うため必要 |
| | 全ての記録項目 | 別添2を参照。 |
| ⑤保有開始日 | | 平成29年1月1日 |
| ⑥事務担当部署 | | 健康福祉局　長寿社会部　医療年金課 |

| 3. 特定個人情報の入手・使用 | | |
|---|---|---|
| ①入手元 ※ | | [ ○ ] 本人又は本人の代理人<br>[ ○ ] 評価実施機関内の他部署 （ 戸籍住民課、市民税管理課、生活援護管理課、国民健康保険課 ）<br>[ ○ ] 行政機関・独立行政法人等 （ 日本年金機構 ）<br>[ ] 地方公共団体・地方独立行政法人 （ ）<br>[ ] 民間事業者 （ ）<br>[ ] その他 （ ） |
| ②入手方法 | | [ ○ ] 紙 [ ○ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ<br>[ ] 電子メール [ ] 専用線 [ ○ ] 庁内連携システム<br>[ ] 情報提供ネットワークシステム<br>[ ○ ] その他 （ データベースを直接参照 ） |
| ③入手の時期・頻度 | | 入手元：本人または本人の代理人<br>【被保険者情報】【受給権者情報】<br>本人からの届書や申請書・年金請求書の提出があった都度<br><br>入手元：評価実施機関内の他部署<br>【住民基本台帳情報】<br>異動があった都度、庁内連携システムにより入手<br>【個人住民税関係情報】【生活保護受給情報】<br>月1回庁内連携システムにより入手、又は、年1回保険年金システムから入手<br><br>入手元：行政機関・独立行政法人<br>【日本年金機構】<br>随時、日本年機構から送付される処理結果一覧等により入手 |
| ④入手に係る妥当性 | | 国民年金第1号被保険者の加入手続・種別変更や、保険料免除等申請、年金請求等を受理し、日本年金機構に個人番号を含めた異動情報を報告するため、入手が必要。国民年金保険料免除申請時における審査に関する事務を行うため、入手が必要。 |
| ⑤本人への明示 | | ・本人及び日本年金機構から入手する情報については、国民年金関係法令で定められる。<br>・庁内連携を通じた入手については、番号法及び条例で定められる。 |
| ⑥使用目的 ※ | | ・被保険者・受給者からの届出や申請、又は請求の受理並びに日本年金機構への送付。<br>・日本年金機構からの被保険者・受給者に関する処理結果管理。 |
| | 変更の妥当性 | |
| ⑦使用の主体 | 使用部署 ※ | 健康福祉局 長寿社会部 医療年金課 及び 各区保険年金課 |
| | 使用者数 | [ 50人以上100人未満 ]<br><選択肢><br>1）10人未満 2）10人以上50人未満<br>3）50人以上100人未満 4）100人以上500人未満<br>5）500人以上1,000人未満 6）1,000人以上 |

| | | |
|---|---|---|
| ⑧使用方法 ※ | | 1. 国民年金被保険者の資格管理にかかる事務<br>被保険者からの届出や住民異動情報、厚生年金等の加入・喪失情報により資格要件確認を行い、受付処理および資格異動情報の管理・日本年金機構へ異動情報の送付を行う。<br><br>2. 国民年金保険料免除等申請にかかる事務<br>被保険者からの免除等申請を受理し、世帯・所得情報などの審査を行い、申請書を日本年金機構へ送付する。<br><br>3. 老齢基礎・障害基礎・遺族基礎年金等の年金請求及び受給権者からの届出にかかる事務<br>年金請求又は届出にかかる受付・所得情報の審査を行い、請求書等を日本年金機構へ送付する。<br><br>4. 対象者(被保険者・受給権者)の承認結果等入力にかかる事務<br>日本年金機構から送付される処理結果一覧等を受理し、結果入力・管理を行う。 |
| | 情報の突合 ※ | 本人の申請内容及び本人確認書類や添付書類等と、住基情報又は税情報を突合し、被保険者情報を確認する。 |
| | 情報の統計分析 ※ | 個人番号を用いた統計分析は行わない。 |
| | 権利利益に影響を与え得る決定 ※ | ・国民年金保険料免除等の審査を行い、日本年金機構が決定を行う。<br>・老齢基礎・障害基礎・遺族基礎年金などの年金請求に関する審査を行い、日本年金機構が決定を行う。 |
| ⑨使用開始日 | | 平成29年1月1日 |
| **4. 特定個人情報ファイルの取扱いの委託** | | |
| 委託の有無 ※ | | [ 委託する ] <選択肢><br>1) 委託する 2) 委託しない<br>( 3 ) 件 |
| **委託事項1** | | システムの運用保守業務及び標準準拠システムへの移行に伴うデータ抽出業務並びに標準準拠システム構築業務 |
| ①委託内容 | | システムの運用保守業務及び標準準拠システムへの移行に伴うデータ抽出業務並びに標準準拠システムを構築する業務を行うにあたり、必要な範囲で特定個人情報ファイルの取扱いを委託 |
| ②取扱いを委託する特定個人情報ファイルの範囲 | | [ 特定個人情報ファイルの全体 ] <選択肢><br>1) 特定個人情報ファイルの全体<br>2) 特定個人情報ファイルの一部 |
| | 対象となる本人の数 | [ 10万人以上100万人未満 ] <選択肢><br>1) 1万人未満<br>2) 1万人以上10万人未満<br>3) 10万人以上100万人未満<br>4) 100万人以上1,000万人未満<br>5) 1,000万人以上 |
| | 対象となる本人の範囲 ※ | 国民年金被保険者及びその世帯員、受給権者及びその世帯員、過去に本市に住民登録のあった被保険者等であった者 |
| | その妥当性 | システムトラブルの調査・復旧、その他保全に関する作業において、特定個人情報ファイルの全体を取扱う必要があるため |
| ③委託先における取扱者数 | | [ 10人以上50人未満 ] <選択肢><br>1) 10人未満 2) 10人以上50人未満<br>3) 50人以上100人未満 4) 100人以上500人未満<br>5) 500人以上1,000人未満 6) 1,000人以上 |
| ④委託先への特定個人情報ファイルの提供方法 | | [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体(フラッシュメモリを除く。)<br>[ ] フラッシュメモリ [ ] 紙<br>[ ○ ] その他 ( 堺市役所庁舎設置のサーバー内又は端末機内及びガバメントクラウド内での提供 ) |
| ⑤委託先名の確認方法 | | 堺市ホームページの委託業務入札結果・随意契約結果一覧に公表している |
| ⑥委託先名 | | 株式会社日立製作所 |

| | | |
|---|---|---|
| 再委託 | ⑦再委託の有無 ※ | [　　再委託する　　] ＜選択肢＞ 1）再委託する　2）再委託しない |
| | ⑧再委託の許諾方法 | 業務の一部を再委託する場合については、契約書により以下の条件を課している。<br>・委託先は、個人情報取扱に係る事項について委託先同様の義務を再委託先に負わせ、再委託先に対し遵守を監督すること。<br>・再委託先事業者から委託先事業者に提出される個人情報等の保護に係る誓約書の写しを本市に提出すること。<br>・再委託先従事者から再委託先事業者に提出される秘密保持に関する誓約書の写しを本市に提出すること。<br>・再委託先の業務従事者に対するセキュリティ等に関する社員教育の実績書及び計画書を本市に提出すること。<br>また再委託の許諾については本市に提出される再委託申請書を以下の観点から審査した上で、判断する。<br>―再委託先の名称、所在地、連絡先電話番号が、正確に記載されていること。<br>―再委託が、業務の一部かつ専門的な作業であること。<br>―再委託する作業内容を具体的に明記していること。<br>―全部又は大部分の再委託でないこと。 |
| | ⑨再委託事項 | 業務の一部 |
| **委託事項2** | | パンチ委託業務 |
| ①委託内容 | | 日本年金機構から送付される処理結果一覧表等、国民年金システムに反映させる紙媒体上の情報を、パンチ委託によりデータ化してシステム内に取込む。 |
| ②取扱いを委託する特定個人情報ファイルの範囲 | | [ 特定個人情報ファイルの一部 ] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部 |
| | 対象となる本人の数 | [　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上 |
| | 対象となる本人の範囲 ※ | 本市に住民登録がある20歳到達予定者及び国民年金被保険者 |
| | その妥当性 | 日本年金機構から送付される被保険者情報を、堺市で登録・保管するため、電子化して国民年金システムに取込む必要がある。 |
| ③委託先における取扱者数 | | [　　10人以上50人未満　　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上 |
| ④委託先への特定個人情報ファイルの提供方法 | | [　]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。）<br>[　]フラッシュメモリ　[ ○ ]紙<br>[　]その他　（　　） |
| ⑤委託先名の確認方法 | | 情報提供にて対応する |
| ⑥委託先名 | | 株式会社エス・ピー・シー |
| 再委託 | ⑦再委託の有無 ※ | [　　再委託しない　　] ＜選択肢＞ 1）再委託する　2）再委託しない |
| | ⑧再委託の許諾方法 | |
| | ⑨再委託事項 | |

| | | |
|---|---|---|
| **委託事項3** | | 統合利用番号連携サーバー、共通基盤システム等に関するシステム保守 |
| ①委託内容 | | 統合利用番号連携サーバー、共通基盤システム等のパッケージアプリケーション保守作業、職員からの問い合わせに対する調査等を行う。 |
| ②取扱いを委託する特定個人情報ファイルの範囲 | | [ 特定個人情報ファイルの一部 ]　＜選択肢＞<br>1）特定個人情報ファイルの全体<br>2）特定個人情報ファイルの一部 |
| | 対象となる本人の数 | [ 10万人以上100万人未満 ]　＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| | 対象となる本人の範囲 ※ | 堺市に住民登録のある国民年金第1号被保険者 |
| | その妥当性 | 庁内連携又は情報提供ネットワークシステムでの他機関連携実施に必要なデータを当該システムに連携する必要がある。 |
| ③委託先における取扱者数 | | [ 10人未満 ]　＜選択肢＞<br>1）10人未満　2）10人以上50人未満<br>3）50人以上100人未満　4）100人以上500人未満<br>5）500人以上1,000人未満　6）1,000人以上 |
| ④委託先への特定個人情報ファイルの提供方法 | | [ ○ ]専用線　[ ]電子メール　[ ]電子記録媒体（フラッシュメモリを除く。）<br>[ ]フラッシュメモリ　[ ]紙<br>[ ]その他　（　） |
| ⑤委託先名の確認方法 | | 委託先が決定後、公告を掲示し公表する。 |
| ⑥委託先名 | | 富士通株式会社 |
| 再委託 | ⑦再委託の有無 ※ | [ 再委託する ]　＜選択肢＞<br>1）再委託する　2）再委託しない |
| | ⑧再委託の許諾方法 | 業務の一部を再委託する場合については、契約書により以下の条件を課している。<br>・委託先は、個人情報取扱に係る事項について委託先同様の義務を再委託先に負わせ、再委託先に対し遵守を監督すること。<br>・再委託先事業者から委託先事業者に提出される個人情報等の保護に係る誓約書の写しを本市に提出すること。<br>・再委託先従事者から再委託先事業者に提出される秘密保持に関する誓約書の写しを本市に提出すること。<br>・再委託先の業務従事者に対するセキュリティ等に関する社員教育の実績書及び計画書を本市に提出すること。<br>また再委託の許諾については本市に提出される再委託申請書を以下の観点から審査した上で、判断する。<br>—再委託先の名称、所在地、連絡先電話番号が、正確に記載されていること。<br>—再委託が、業務の一部かつ専門的な作業であること。<br>—再委託する作業内容を具体的に明記していること。<br>—全部又は大部分の再委託でないこと。<br>—再委託する作業内容に関して、契約の履行に必要な専門的な作業の実績又は堺市若しくは他の自治体における対象業務の実績を有していること。 |
| | ⑨再委託事項 | 共通基盤システム保守業務及び統合利用番号連携サーバーにかかる随時作業及び運用設計作業 |

| 5. 特定個人情報の提供・移転（委託に伴うものを除く。） | |
|---|---|
| 提供・移転の有無 | [ ○ ] 提供を行っている （ 1 ）件 [ ○ ] 移転を行っている （ 1 ）件<br>[ ] 行っていない |
| **提供先1** | 厚生労働大臣（日本年金機構） |
| ①法令上の根拠 | 番号法第9条第1項別表第一 第31の項 |
| ②提供先における用途 | ・国民年金第1号被保険者に関する異動情報の登録<br>・国民年金保険料免除等申請、年金請求等にかかる審査・決定 |
| ③提供する情報 | ・国民年金第1号被保険者に関する異動情報<br>・国民年金保険料免除等申請、年金請求等にかかる審査・決定に必要な情報 |
| ④提供する情報の対象となる本人の数 | [ 10万人以上100万人未満 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| ⑤提供する情報の対象となる本人の範囲 | ・被保険者及びその世帯員<br>・年金請求者及びその世帯員 |
| ⑥提供方法 | [ ] 情報提供ネットワークシステム [ ] 専用線<br>[ ] 電子メール [ ○ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ○ ] 紙<br>[ ] その他 （ ） |
| ⑦時期・頻度 | 毎日 |
| **移転先1** | 市民人権局 市民生活部 戸籍住民課 |
| ①法令上の根拠 | 住民基本台帳法第七条第11号 |
| ②移転先における用途 | 住民票への記載 |
| ③移転する情報 | 国民年金の被保険者となった年月日、又は被保険者でなくなった年月日、被保険者の種別及びその変更があった年月日、基礎年金番号 |
| ④移転する情報の対象となる本人の数 | [ 10万人以上100万人未満 ]<br>＜選択肢＞<br>1）1万人未満<br>2）1万人以上10万人未満<br>3）10万人以上100万人未満<br>4）100万人以上1,000万人未満<br>5）1,000万人以上 |
| ⑤移転する情報の対象となる本人の範囲 | 堺市に住民登録のある国民年金第1号被保険者 |
| ⑥移転方法 | [ ○ ] 庁内連携システム [ ] 専用線<br>[ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。）<br>[ ] フラッシュメモリ [ ] 紙<br>[ ] その他 （ ） |
| ⑦時期・頻度 | 週1回 |

## 6. 特定個人情報の保管・消去

| | | |
|---|---|---|
| ①保管場所 ※ | | 1. 保管場所の態様<br>堺市情報セキュリティ対策基準要綱第9条（サーバーの導入及び運用）に規定される「（1）サーバーは、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置しなければならない。」及び第11条（管理区域）に規定する「（1）水害対策及び確実な入退室管理を行うこと。」に基づき、以下の対策を行っている。<br>・保管場所は堺市役所本館9階にある無窓の電算機室に設置している。<br>・電算機室内のサーバー等は、落下しないようにベルトを掛け、又はビス止めするなど転倒及び落下防止等の耐震対策を行っている。<br>・電算機室に火災報知器や消火設備等を設置するなどの防火措置を行っている。<br>・電算機室に漏水センサーを設置するなどの防水措置を行っている。<br>・電算機室から外部に通ずるドアは最小限とし、入口には監視カメラを設置している。<br><br>2. 保管場所への立入制限・アクセス制限<br>堺市情報セキュリティ対策基準要綱第9条（サーバーの導入及び運用）に規定する「（4）操作の権限を有しない者に容易に操作されることがないよう、サーバーに記録された情報の重要度に応じて設置場所への入室制限を行うなど適切な措置を講じなければならない。」に基づき、以下の対策を行っている。<br>・電算機室への入室は許可された者のみが必要な区画のみに立ち入るように制限し、ICカードによる入退室管理を行っている。<br>・入室者は、電算機室に入室する場合、身分証明書等を携帯している。<br>・あらかじめ入室許可を受けていないものが障害等の突発的対応によって電算機室に入る場合は、同室への入室を許可された職員等が付き添うものとし、外見上職員等と区別できるようにしている。<br>・サーバー等は施錠できるラックに格納し、第三者による不正操作を防止している。<br><br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 |
| ②保管期間 | 期間 | ［　　20年以上　　］<br>＜選択肢＞<br>1）1年未満　2）1年　3）2年<br>4）3年　5）4年　6）5年<br>7）6年以上10年未満　8）10年以上20年未満　9）20年以上<br>10）定められていない |
| | その妥当性 | 年金業務においては、遺族年金の支給等のため本人の死後も含めて長期間にわたって記録を管理する必要があることから、厚生労働省（日本年金機構）において、記録の保管期間を定めず恒久的に保管することとしている。このことから、法定受託事務を行う市町村で受付けた記録等についても、同様に長期間保管する必要があるため保管期間は定められていないが、住民基本台帳法施行令第34条（住民票が消除された日から5年間保存）に基づき、本市の住民基本台帳から削除された者については、国民年金システムの記録においても削除する。 |
| ③消去方法 | | 堺市情報セキュリティ対策基準要綱第8条（記録媒体の管理）に規定する「(5)不要となった記録媒体を廃棄する場合は、データ管理者の許可を得なければならない。この場合において、不要となった記録媒体については、当該媒体に含まれる情報をいかなる方法によっても復元することができないように消去等を行ったうえで、廃棄しなければならない。」及び「(6)重要な情報を記録した記録媒体の廃棄については、その重要度に応じて、日時、処理担当者及び処理内容を記録するなど適切な処理を行わなければならない。」に基づき、以下の対策を行っている。<br>・国民年金システムにおいては、年金情報を一括削除する機能を設けており、不要になった情報については、データ管理者の許可のもと、年1回のサイクルで、復元不可能な状態での削除処理を行う。<br><br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は本市からの操作によって実施される。本市の業務データは国及びガバメントクラウドのクラウド事業者にはアクセス制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27001等にしたがって確実にデータ消去する。<br>③既存システムについては、本市が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 |

## 7. 備考

| |
|---|
| |

## （別添2）特定個人情報ファイル記録項目

別紙のとおり

# 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 ※（7. リスク1⑨を除く。）

| 1. 特定個人情報ファイル名 | |
|---|---|
| 年金情報ファイル | |
| **2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）** | |
| リスク1：　目的外の入手が行われるリスク | |
| 対象者以外の情報の入手を防止するための措置の内容 | ・届出窓口において、届出内容や本人確認書類の確認を厳格に行い、対象者以外の個人情報を入手することのないようにする。<br>・窓口での届出内容や、日本年金機構から送付される処理結果一覧表の情報を、国民年金システムへ入力後、システムから出力した照合用リストにより、入力間違いがないか、届出書との内容照合を行う。<br>・他の機関及び庁内連携を通じて入手する際も、入手元とあらかじめ対象者の関連付けを行っておくことにより、対象者以外の情報を入手できないようにしている。 |
| 必要な情報以外を入手することを防止するための措置の内容 | ・届出窓口において、届出内容や本人確認書類の確認を厳格に行い、対象者又は対象者以外の、必要でない情報を入手することのないようにする。<br>・窓口での届出内容や日本年金機構から送付される処理結果一覧表の情報を、国民年金システムへ入力後、システムから出力した照合用リストにより、入力間違いがないか届出書との内容照合を行う。<br>・所属長が業務上の必要性を考慮上、ユーザ登録の依頼を行い、権限者はその必要性を十分確認したうえで登録を行っている。<br>・登録されたユーザには本人のみが知り得るパスワードを設定し、登録外の者が利用できないよう制限している。<br>・アクセスする権限を各画面で設定し、業務に必要な画面以外はアクセスできないように制限している。<br>・ユーザIDの取扱い等について、離席時のログアウトの徹底等の運用ルールを定めている。 |
| その他の措置の内容 | |
| リスクへの対策は十分か | [　十分である　] ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| リスク2：　不適切な方法で入手が行われるリスク | |
| リスクに対する措置の内容 | ・所属長は、利用者抹消（人事異動、出向、退職等）の状況が発生した際は、速やかにユーザ削除の依頼を行うこと、権限者は速やかに削除の処理を行うよう運用ルールを定めている。<br>・所属長がユーザ削除の依頼を行い、権限者はその内容を十分確認したうえで削除を行っている。<br>・当該業務に関係のない情報を入手できないよう、システム的に制限している。 |
| リスクへの対策は十分か | [　十分である　] ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| リスク3：　入手した特定個人情報が不正確であるリスク | |
| 入手の際の本人確認の措置の内容 | 窓口において、対面で本人確認書類による本人確認作業を行う。 |
| 個人番号の真正性確認の措置の内容 | 窓口において、個人番号カード若しくは身分証明書等で、個人番号の真正性確認を行う。真正性に疑問がある場合は、随時、住基情報所管部署に問い合わせを行う。 |
| 特定個人情報の正確性確保の措置の内容 | 窓口で入手した情報については、本人への聞き取りや住基情報、本人確認書類や添付書類との照合を行い、正確性を確保する。 |
| その他の措置の内容 | |
| リスクへの対策は十分か | [　十分である　] ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| リスク4：　入手の際に特定個人情報が漏えい・紛失するリスク | |
| リスクに対する措置の内容 | ・窓口で特定個人情報を入手する際は、他の来庁者の覗き込み等ができないよう、カウンターに間仕切りを設置して対応し、対応時のメモは、速やかにシュレッダー処理を行う。<br>・申請書類等は、特定個人情報の漏洩及び紛失防止のため、施錠可能な書庫に保管する。<br>・国民年金システムは、インターネットと直接接続していない。 |
| リスクへの対策は十分か | [　十分である　] ＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
| | |

| 3. 特定個人情報の使用 | | |
|---|---|---|
| リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク | | |
| 宛名システム等における措置の内容 | | 国民年金業務では宛名システムは使用しない。 |
| 事務で使用するその他のシステムにおける措置の内容 | | 他のシステムからは、個人番号を伴う情報はアクセスできないようにシステムが構築されている。 |
| その他の措置の内容 | | |
| リスクへの対策は十分か | | [ 特に力を入れている ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク | | |
| ユーザ認証の管理 | | [ 行っている ] ＜選択肢＞<br>1）行っている 2）行っていない |
| | 具体的な管理方法 | 1. ユーザの認証方法<br>堺市情報セキュリティ対策基準要綱第13条（職員の責務）第3項に規定する「（9）操作を許可された者以外に端末機もしくはサーバーの操作方法を教示し、又は端末機もしくはサーバーの操作をさせないこと。」に基づき、以下の対策を行っている。<br><br>ユーザ認証は3段階で実施している。業務システムを利用するときは、まずWindowsログイン認証前に生体（顔）による認証を行い、次に共通基盤システムのディレクトリサービス機能において、許可された個人ごとに付与したユーザIDとパスワードにより、個人ごとのWindowsログイン認証を行う二要素認証を実施している。次に、ログインした端末から業務システムを利用する際は、Windowsログインのユーザを利用したシングルサインオンを実施している。<br><br>2. なりすましが行われないための対策<br>堺市情報セキュリティ対策基準要綱第13条（職員の責務）第4項に規定する「（1）他人に自己の保有するIDを使用させないこと。」「（2）自己の保有するパスワードに関し、他に知られないよう適切な管理を行うこと。」「（3）パスワードは、十分な長さのもので第三者が想像しにくいものとすること。」「（4）パスワードは、定期的に変更すること。」「（5）端末機及びサーバにパスワードを記憶させないこと。」に基づき、以下の対策を行っている。<br><br>・ユーザIDについて<br>−職員等は、自己が利用しているIDを他人に利用させないこととしている。<br>・パスワードについて<br>−職員等は、パスワードの照会等には一切応じない、パスワードのメモを机上等に置かない等の対策により、他者に知られないように管理している。<br>−職員等は、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のみを設定できるようにしている。<br>−職員等は、パスワードが流出したおそれがある場合には、電算管理者にすみやかに報告し、パスワードを速やかに変更している。<br>−システムログイン時に、パスワードの変更を促し、以降定期的にパスワードの変更を要求している。<br>−職員等はパスワードは定期的に変更し、古いパスワードを再利用しないこととしている。<br>−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共有しないこととしている。<br>−職員等の仮のパスワードは、最初のログイン時点で変更している。<br>−職員等は、端末にパスワードを記憶させないこととしている。<br>−職員等間でパスワードを共有しないこととしている。<br><br>・共通基盤システムのWindowsログイン認証において、パスワードは一定以上の長さとすることが必須となっており、自己により随時変更可能である。<br>・共通基盤システムのWindowsログイン認証において、初回パスワードは、初回ログイン時に強制的に変更している。<br>・共通基盤システムのWindowsログイン認証において、パスワードは強制的に一定期間ごとに変更している。<br>・共通基盤システムのWindowsログイン認証において、パスワード変更時は前回使用のパスワードに変更することはできないようになっている（継続使用不可）。<br>・共通基盤システムのWindowsログイン認証前に生体（顔）による認証を行うことにより、なりすましが行われないよう講じている。 |

| | | |
|---|---|---|
| アクセス権限の発効・失効の管理 | | [　行っている　] ＜選択肢＞ 1）行っている　2）行っていない |
| | 具体的な管理方法 | 堺市情報セキュリティ対策基準要綱第17条（アクセス制御）第1項に規定する「（1）情報システムを利用する職員等について、情報システムごとに定められた方法に従い、その登録、変更、抹消等を行うこと」に基づき、以下の対策を行っている。<br><br>〇発行管理<br>【国民年金システム】<br>・各所属の所属長が業務上の必要性を考慮の上、ユーザ登録の依頼を行い、権限者はその必要性を十分確認したうえで登録を行っている。<br>・登録されたユーザには本人のみが知り得るパスワードを設定し、登録外の者が利用できないよう制限している。<br>・アクセスする権限を各画面で設定し、業務に必要な画面以外はアクセスできないように制限している。<br>・ユーザIDの取扱い等について、離席時のログアウトの徹底等の運用ルールを定めている。<br><br>【共通基盤システム】<br>・所属長がICTイノベーション推進室にユーザ登録依頼を行い、ICTイノベーション推進室にて必要なWindowsログインに係るアクセス権限を付与している。 |
| アクセス権限の管理 | | [　行っている　] ＜選択肢＞ 1）行っている　2）行っていない |
| | 具体的な管理方法 | 堺市情報セキュリティ対策基準要綱第１７条（アクセス制御）第1項に規定している「(3) 情報システムの管理に係る権限の付与は、必要最小限の者に限ることとし、厳重に管理すること。」に基づき、以下の対策を行っている。<br><br>・利用されていないIDが放置されないよう、人事情報をもとに定期的に点検している。<br>・年度当初の業務体制変更時や配置換え等が発生した際に、各従事者ごとの割当内容を所属長が確認している。<br><br>共通基盤システムにおいて、以下のとおり、アクセス権限の管理を行っている。<br>・ディレクトリサービス機能において、操作者の業務内容に応じた最低限のアクセス権限が付与されるように管理している。<br>・利用していないIDが放置されないよう、システム所管課において、操作者の業務内容に応じた最低限のアクセス権限が付与されることを年次で確認している。 |
| 特定個人情報の使用の記録 | | [　記録を残している　] ＜選択肢＞ 1）記録を残している　2）記録を残していない |
| | 具体的な方法 | 堺市情報セキュリティ対策基準要綱第１６条（電子計算機及びネットワークの管理）第1項に規定する「(1) 各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、不正なアクセス等に対処できるよう一定の期間保存し、及び記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずること。」に基づき、以下の対策を行っている。<br><br>・情報システムの運用において実施した作業について、ログを作成している。<br>・各種アクセス記録及び情報セキュリティの確保に必要な記録（利用者、端末機、操作日時、操作内容等）を取得し、一定期間保存している。<br>・アクセス記録等が詐欺、改ざん、誤消去等されないように、操作権限は必要最低限の人数にしか与えないなどの必要な措置を講じている。<br>・個人を特定した検索および特定後の異動処理や帳票印刷などの操作ログの記録を行っている。<br><br>共通基盤システムにおいて、以下のとおり、特定個人情報の使用の記録を行っている。<br>・ディレクトリサービス機能において、いつ、どの端末で、誰が、ネットワークにログイン/ログアウトしたかを記録し、一定期間保存している。<br>・データ連携機能により特定個人情報ファイルにアクセスしたログ（いつ、どのシステムが）を取得し、一定期間保存している。 |
| その他の措置の内容 | | |
| リスクへの対策は十分か | | [　特に力を入れている　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている |

| | |
|---|---|
| リスク3： 従業者が事務外で使用するリスク | |
| リスクに対する措置の内容 | 1. 教育・啓発<br>・年1回、J-LISの「e-Learningによる情報セキュリティ研修」を実施し、本市における、個人情報の取扱い等に関する一般知識の習得及び意識レベルの向上に取り組んでいる。<br>・年1回、各課で選任されている情報セキュリティ担当者を対象に、「情報セキュリティの普及・啓発に係る取組み」に必要な知識の習得を目的とした研修を実施している。<br>・毎年度、新任管理職及び新規採用の職員等を対象とした、情報セキュリティに関する研修を実施している。<br><br>2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第10項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。<br>・違反行為を行ったものに対しては、違反行為の程度によっては地方公務員法による懲戒の対象としている。 |
| リスクへの対策は十分か | [ 特に力を入れている ]　＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| リスク4： 特定個人情報ファイルが不正に複製されるリスク | |
| リスクに対する措置の内容 | データの抽出（サーバ内への保存）は特定の業務担当者のみの権限としている。<br>外部媒体への出力は特定の管理担当者のみの権限としている。 |
| リスクへの対策は十分か | [ 特に力を入れている ]　＜選択肢＞<br>1）特に力を入れている　2）十分である<br>3）課題が残されている |
| 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 | |
| ・許可のない外部記録媒体が使用できないように制限している。<br>・ファイルの持ち出しについて、持出し申請者を限定するとともに、上長の承認が必要であり、また、上長の承認を得たファイルは、申請した者しか持ち出すことが出来ないように制限している。<br>・いつ、誰が、どの端末で、どのデバイスに、どのファイルを持ち出し、持ち込みしたか、誰が持出し承認したかを記録するとともに、記録を取得していることを関係者に周知し、不正な持出しを抑止している。 | |
| **4. 特定個人情報ファイルの取扱いの委託** | **[ ] 委託しない** |
| 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<br>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<br>委託先による特定個人情報の保管・消去に関するリスク<br>委託契約終了後の不正な使用等のリスク<br>再委託に関するリスク | |
| 情報保護管理体制の確認 | 業者選定に際しては同等業務の履行実績確認を行い、特定個人情報の保護を適切に行える委託先であることを確認する。契約時には個人情報等の保護に係る誓約書、業務従事者届、業務従事者の経歴書、業務従事者からの秘密保持に関する誓約書、実施体制図、セキュリティ等に関する社員教育の実績書及び計画書、堺市暴力団排除条例に係る誓約書の提出を義務付けている。 |
| 特定個人情報ファイルの閲覧者・更新者の制限 | [ 制限している ]　＜選択肢＞<br>1）制限している　2）制限していない |
| 具体的な制限方法 | 業務従事者届等の提出時に、委託先と協議を行い適正な従事者数を定める。電算機室の入室に係るシステム管理部門への事前登録は、必要最低限の人数としている。閲覧・更新の操作ログを取得し、不正な使用がないことの確認ができるようにしている。 |
| 特定個人情報ファイルの取扱いの記録 | [ 記録を残している ]　＜選択肢＞<br>1）記録を残している　2）記録を残していない |
| 具体的な方法 | 事務システムの操作ログを全て記録し、7年間保管する。不具合データの調査など、システムによるログの自動取得ができない作業については、所定のサーバー内のフォルダに作業証跡の記録を行う。また、作業終了後に、作業概要と作業者についての報告書を提出させて確認を行う。 |

| | | |
|---|---|---|
| 特定個人情報の提供ルール | | [　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない |
| | 委託先から他者へ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 | 【運用・保守業務】<br>委託に関する作業では、特定個人情報を他者へ提供することを一切認めていない。<br><br>【パンチ業務】<br>契約書上で再委託は認めない旨を明記している。また、同じく、目的外利用の禁止、第三者への提供の禁止を明記している。 |
| | 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 | システムの品質担保等の目的により庁舎外での作業が必要な場合は、個人情報を不可逆なダミーデータに置換をし、市職員の監視を受けた上で持ち出しを行う。 |
| 特定個人情報の消去ルール | | [　　定めていない　　] ＜選択肢＞ 1）定めている　2）定めていない |
| | ルールの内容及びルール遵守の確認方法 | 【運用・保守業務】<br>委託業者にはダミーデータのみを提供しており、特定個人情報の消去の必要性は生じない。<br><br>【パンチ業務】<br>契約書上で許可なく複写、複製することを禁じており、納品時に入力用の帳票とその複写、複製物を併せて納品させることにしている。納品後はパンチ後のデータを削除するよう義務付けている。 |
| 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 | | [　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない |
| | 規定の内容 | 個人情報の取扱いについては、堺市個人情報保護条例に則り、個人情報の保護の重要性を認識し、個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。<br>（規定内容）<br>〇契約終了又は解除された後においても秘密保持すること<br>〇従事者に対して堺市個人情報保護条例で定める罰則の教示を行うこと<br>〇個人情報の収集の制限と適正管理を行うこと<br>〇目的外の使用と第三者への提供の禁止<br>〇個人情報の返還と廃棄に関すること<br>〇事故発生時の速やかな報告<br>〇契約事項の違反による損害賠償の担保 |
| 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 | | [　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 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 | 再委託先は、その相手方、理由に本市の承認があるもののみを許可している。<br>また、委託先と同様の義務を負わせ、その順守を監督することを委託契約書において特記事項として定めている。 |
| その他の措置の内容 | | |
| リスクへの対策は十分か | | [　　十分である　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 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 | | |
| | | |

| 5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。） | [　　]提供・移転しない |
|---|---|
| リスク1： 不正な提供・移転が行われるリスク | |
| 特定個人情報の提供・移転の記録 | [　　記録を残している　　]　＜選択肢＞ 1）記録を残している　2）記録を残していない |
| 具体的な方法 | ○共通基盤システムによる情報の移転<br>移転を行う情報をあらかじめ仕様にて取り決め、住民情報の変更データ等を随時自動で提供する仕組みを構築している。仕様で定めた以外の情報の抜き取りを各システムから行うことは不可能で、共通基盤システムへの提供ログはシステム内に自動で保管され、刑事訴訟手続上の証拠保全のため、刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存している。随時でデータの移転を行う際は、対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ、詳細を記録している。<br><br>移転を行う場合、移転する情報に関して、移転元と移転先において仕様を定め、所属長の許可を得た上でICTイノベーション推進室に依頼をする。仕様で定めたことのみシステム構築しており、仕様以外の情報に関しては、移転不可能である。どのシステムがどの情報に対して、いつ移転したかをネットワークの通信ログで取得しており、一定期間保存している。正当な移転だけでなく、不正な移転、移転の失敗など全ての通信ログを取得している。 |
| 特定個人情報の提供・移転に関するルール | [　　定めている　　]　＜選択肢＞ 1）定めている　2）定めていない |
| ルールの内容及びルール遵守の確認方法 | ○共通基盤システムによる情報の移転<br>システムの使用を定める際に関係各課と協議を行い、法令上の根拠等を確認した上でシステムを構築し、適切なタイミングで自動で提供する仕組みを構築している。随時で行う際も、その都度不適切な移転でないことを確認し、決裁行為を経た上で行っている。<br><br>特定個人情報の提供・移転に係るルール（規定類）の詳細については、今後公布される政省令等の内容を踏まえて策定することを予定している。 |
| その他の措置の内容 | ・入室権限を厳格に管理している電算機室にサーバーを設置し、情報の持ち出しを制限している。<br>・共通基盤システムにおいて、個人番号管理ファイルを扱うシステムへのアクセス権限を有する者を厳格に管理し、基本的に媒体接続は禁止しており、情報の持ち出しを制限している。<br>・利用するパソコンのハードディスクやUSBメモリ、CDメディアへの書き込みは一般ユーザでは技術的にできなくしている。管理ユーザでは書き込む際は必ず暗号化するしくみを構築し、その内容、実施日、理由を台帳管理している。<br>・遠隔地保管を行うバックアップ用LTOメディアの運送業者への受渡しは記録簿にて管理を行っている。 |
| リスクへの対策は十分か | [　　特に力を入れている　　]　＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている |
| リスク2： 不適切な方法で提供・移転が行われるリスク | |
| リスクに対する措置の内容 | ・移転を行う情報をあらかじめ仕様にて取り決め、住民情報の変更データ等を随時自動で提供する仕組みを構築している。仕様で定めた以外の情報の抜き取りを各システムから行うことは不可能で、共通基盤システムへの提供ログはシステム内に自動で保管されている。<br>・随時でデータの移転を行う際は、対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ、詳細を記録している。媒体にて他課に移転する際は、パスワードの付与を行い、第三者への漏洩を防止している。<br>・連携手段として情報連携の記録が逐一保存され、不適切な方法による特定個人情報の提供を防止している。<br>・許可のない外部記録媒体が使用できないように制限している。<br>・ファイルの持ち出しについて、持出し申請者を限定するとともに、上長の承認が必要であり、また、上長の承認を得たファイルは、申請した者しか持ち出すことが出来ないように制限している。<br>・いつ、誰が、どの端末で、どのデバイスに、どのファイルを持ち出し、持ち込みしたか、誰が持出し承認したかを記録するとともに、記録を取得していることを関係者に周知し、不正な持出しを抑止している。 |
| リスクへの対策は十分か | [　　特に力を入れている　　]　＜選択肢＞ 1）特に力を入れている　2）十分である　3）課題が残されている |

| | |
|---|---|
| リスク3： 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク | |
| リスクに対する措置の内容 | 【データ連携】<br>・情報の提供はほとんどが共通基盤システムを介した自動によるものである。<br>・随時の場合は手作業となるが、対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ、誤りのデータを直接手渡し、又は、暗号化及びセキュアな通信方法によるものとしている。<br>・共通基盤システムにおいて、連携データごとにデータ種別、通信相手ごとに持つIDとパスワードを取り決め、認証行為を行っている。<br>【オンライン利用】<br>・個人単位でIDとパスワードを取り決め、認証行為を行った上で、必要な情報に限定して連携している。 |
| リスクへの対策は十分か | [ 特に力を入れている ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置 | |
| 情報提供ネットワークシステム（中間サーバー）と各業務個別に連携I/Fを設けるのではなく、庁内の連携を連携サーバーに全て集約することで対策している。 | |

| | |
|---|---|
| **6. 情報提供ネットワークシステムとの接続** | **[ ○ ] 接続しない（入手） [ ○ ] 接続しない（提供）** |
| リスク1： 目的外の入手が行われるリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク2： 安全が保たれない方法によって入手が行われるリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク3： 入手した特定個人情報が不正確であるリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク5： 不正な提供が行われるリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク6： 不適切な方法で提供されるリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |
| リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク | |
| リスクに対する措置の内容 | |
| リスクへの対策は十分か | [ ] ＜選択肢＞<br>1）特に力を入れている 2）十分である<br>3）課題が残されている |

| 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置 | | |
|---|---|---|
| | | |

## 7. 特定個人情報の保管・消去

| リスク1： 特定個人情報の漏えい・滅失・毀損リスク | | |
|---|---|---|
| ①NISC政府機関統一基準群 | [ 政府機関ではない ] | ＜選択肢＞<br>1）特に力を入れて遵守している　2）十分に遵守している<br>3）十分に遵守していない　4）政府機関ではない |
| ②安全管理体制 | [ 特に力を入れて整備している ] | ＜選択肢＞<br>1）特に力を入れて整備している　2）十分に整備している<br>3）十分に整備していない |
| ③安全管理規程 | [ 特に力を入れて整備している ] | ＜選択肢＞<br>1）特に力を入れて整備している　2）十分に整備している<br>3）十分に整備していない |
| ④安全管理体制・規程の職員への周知 | [ 特に力を入れて周知している ] | ＜選択肢＞<br>1）特に力を入れて周知している　2）十分に周知している<br>3）十分に周知していない |
| ⑤物理的対策 | [ 十分に行っている ] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>3）十分に行っていない |
| 具体的な対策の内容 | 1．サーバー設置場所<br>堺市情報セキュリティ対策基準要綱第9条（サーバーの導入及び運用）に規定する「（4）操作の権限を有しない者に容易に操作されることがないよう、サーバーに記録された情報の重要度に応じて設置場所への入室制限を行うなど適切な措置を講じなければならない。」及び第11条（管理区域）に規定する「（1）水害対策及び確実な入退室管理を行うこと。」に基づき、以下の対策を行っている。<br>・サーバーを設置する電算機室から外部に通ずるドアは最小限とし、ICカードにて立入を制限の上、監視カメラを設置して入退室を監視している。<br><br>2．端末設置場所<br>堺市情報セキュリティ対策基準要綱第10条（端末機及びサーバーの管理）第1項に規定する「システム利用責任者は、執務室等に職員等がいない場合における当該執務室等の施錠等の徹底、端末機、サーバー等の固定その他情報資産の盗難防止のための措置を講じなければならない。」に基づき、以下の対策を行っている。<br>・職員等は、パソコン等の端末について、第三者に使用されること、又は電算管理者の許可なく情報を閲覧されることがないように、離席時の端末のロック等、適切な措置を講じている。<br>・業務終了後は、パソコン等の端末を施錠できるロッカーへ保管し、又はセキュリティワイヤロックを導入し、盗難を防止している。<br><br>3．記録媒体・紙媒体の保管場所<br>堺市情報セキュリティ対策基準要綱第8条（記録媒体の管理）に規定する「（3）重要な情報を記録した記録媒体については、その重要度に応じて、漏洩、滅失、損傷等の防止に備えるなど適切な対策を講じた場所に保管しなければならない。」に基づき、以下の対策を行っている。<br>・情報を記録した記録媒体を保管する場合、施錠可能なロッカーに保管している。<br>・職員等は、記録媒体や情報が印刷された文書等について、第三者に使用されること、又は電算管理者の許可なく情報を閲覧されることがないように容易に閲覧されない場所（施錠可能な事務所内倉庫や保管庫）へ保管している。<br><br>＜ガバメントクラウドにおける措置＞<br>1．ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br><br>2．事前に許可されていない装置等に関しては、外部に持出できないこととしている。 | |
| ⑥技術的対策 | [ 十分に行っている ] | ＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>3）十分に行っていない |

| | | |
|---|---|---|
| | 具体的な対策の内容 | ○不正プログラム対策<br>堺市情報セキュリティ対策基準要綱第19条（不正プログラム対策）第1項に規定する「職員等は、外部から取り入れ、又は外部へ持ち出すデータ、送受信する電子メール等については、不正プログラムチェック（当該データ等にウイルスが含まれているか否かを調べることをいう。）を行うなど、不正プログラムのシステムへの侵入又は外部への拡散その他不正プログラムによるシステム障害等の発生の防止に努めなければならない。」及び第19条（不正プログラム対策）第2項に規定する「電算管理者は、常時不正プログラムに関する情報収集に努め、不正プログラムチェック用の定義ファイル等は常に最新のものに保たなければならない。」に基づき、以下の対策を行っている。<br>・職員等は記録媒体を使う場合、不正プログラム等の感染を防止するために、市が管理している記録媒体のみを利用している。<br>・サーバー及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させている。<br>・不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を施し、常に最新の状態を保っている。<br><br>○不正アクセス対策<br>堺市情報セキュリティ対策基準要綱第17条（アクセス制御）第1項に規定する「（7）本市の外部の組織から本市のネットワーク及び情報システムにアクセスする場合は、直接本市の内部ネットワークに接続させないこと。」に基づき、以下の対策を行っている。<br>・システムは、外部のインターネットと物理的に接続していない。<br><br>堺市情報セキュリティ対策基準要綱第１８条（ネットワーク及び情報システムの監視）第１項に規定する「電算管理者は、セキュリティに関する事案を検知するため、情報システムについて監視等を行わなければならない。」に基づき、以下の対策を行っている。<br>・電算管理者はセキュリティに関する事案を検知するため、情報システムを常時監視し、障害が起きた際にも速やかに対応できるようにしている。<br><br>＜ガバメントクラウドにおける措置＞<br>1．国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br><br>2．地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。<br><br>3．クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。<br><br>4・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 |
| ⑦バックアップ | | ［　特に力を入れて行っている　］　＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>3）十分に行っていない |
| ⑧事故発生時手順の策定・周知 | | ［　特に力を入れて行っている　］　＜選択肢＞<br>1）特に力を入れて行っている　2）十分に行っている<br>3）十分に行っていない |
| ⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか | | ［　発生あり　］　＜選択肢＞<br>1）発生あり　2）発生なし |
| | その内容 | 受託業者が、長屋建て住宅の所有者を対象とした調査を行った、アンケート調査票に所有者本人以外の氏名を誤って印字した調査票を誤送付（1,461件の個人情報が漏洩） |
| | 再発防止策の内容 | ・受託業者に対し、個人情報を取り扱う場合のマニュアルやチェックリストと、十分な確認が必要な作業の場合、市からの指示に基づく手順書を作成させることにより、個人情報の適正管理、適正な事務処理について、指導と確認を徹底した。<br>・市として、再びこのような事案が発生しないよう、個人情報保護の重要性を再認識し、個人情報を取り扱う作業の場合、受託業者に対し、書面により詳細な作業手順や注意点を明確に指示し、漏洩や手順の誤りがないことの確認を徹底した。 |

| | | |
|---|---|---|
| ⑩死者の個人番号 | | [　　保管している　　] ＜選択肢＞ 1）保管している　2）保管していない |
| | 具体的な保管方法 | 生存者と同様 |
| その他の措置の内容 | | 関係規定の整備<br>メール送信によるインシデント発生を防ぐため、個人情報を含む重要な情報を送信する際のメール使用の是非を慎重に判断するよう関係規定（堺市情報セキュリティポリシー）を改正した。 |
| リスクへの対策は十分か | | [　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている |
| リスク2： 特定個人情報が古い情報のまま保管され続けるリスク | | |
| リスクに対する措置の内容 | | 個人番号は業務上必要とするタイミングで適宜更新され、かつ、それ以外での更新はないため、当該リスクは存在しない。 |
| リスクへの対策は十分か | | [　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている |
| リスク3： 特定個人情報が消去されずいつまでも存在するリスク | | |
| 消去手順 | | [　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない |
| | 手順の内容 | システム上、保管期間の経過した特定個人情報を一括して削除する仕組みとする。<br><br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 |
| その他の措置の内容 | | |
| リスクへの対策は十分か | | [　　特に力を入れている　　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている |
| 特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置 | | |
| | | |

## Ⅳ　その他のリスク対策 ※

| 1. 監査 | | |
|---|---|---|
| ①自己点検 | | [　　十分に行っている　　] ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| | 具体的なチェック方法 | ・J-LISの自己点検シートを参考に、堺市の実情に合わせた自己点検シートを作成し、年1回、職員による自己点検を実施している。また、評価書の記載したとおりに運用がなされているかも確認している。 |
| ②監査 | | [　　十分に行っている　　] ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| | 具体的な内容 | 堺市情報セキュリティ対策基準要綱第24条（監査）第1項に規定する「情報セキュリティ監査統括責任者は、十分な専門的知識を有する者をして情報セキュリティについての監査を定期的にさせなければならない。」に基づき、以下の対応を行っている。<br>・定期的に、外部の第三者による監査を実施している。<br>・監査事項は以下のとおり<br>　-組織のセキュリティ<br>　-人的セキュリティ<br>　-物理的及び環境的セキュリティ<br>　-通信及び運用管理<br>　-アクセス制御<br>　-システムの開発及び保守<br>・監査の実施体制は以下のとおり。<br>　-監査責任者　1名<br>　-監査人　2名<br>・監査結果を踏まえて、当該事項への対処及び実施手順の見直し等に活用している。<br><br>＜ガバメントクラウドにおける措置＞<br>ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 |
| **2. 従業者に対する教育・啓発** | | |
| 従業者に対する教育・啓発 | | [　　十分に行っている　　] ＜選択肢＞<br>1) 特に力を入れて行っている　2) 十分に行っている<br>3) 十分に行っていない |
| | 具体的な方法 | 1. 教育・啓発<br>・年1回、J-LISの「e-Learningによる情報セキュリティ研修」を実施し、本市における、個人情報の取扱い等に関する一般知識の習得及び意識レベルの向上に取り組んでいる。<br>・年1回、各課で選任されている情報セキュリティ担当者を対象に、「情報セキュリティの普及・啓発に係る取組み」に必要な知識の習得を目的とした研修を実施している。<br>・毎年度、新任管理職及び新規採用の職員等を対象とした、情報セキュリティに関する研修を実施している。<br><br>2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第10項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。<br>・違反行為を行ったものに対しては、違反行為の程度によっては地方公務員法による懲戒の対象としている。 |

## 3. その他のリスク対策

＜ガバメントクラウドにおける措置＞ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。

# Ⅴ　開示請求、問合せ

| 1. 特定個人情報の開示・訂正・利用停止請求 | |
|---|---|
| ①請求先 | 堺市　市長公室　広報戦略部　市政情報課<br>〒590-0078　堺市堺区南瓦町3番1号　072-228-7439 |
| ②請求方法 | 指定様式による書面の提出により開示・訂正・削除・中止請求を受付ける。 |
| 特記事項 | |
| ③手数料等 | [　　無料　　]　　＜選択肢＞<br>1) 有料　　2) 無料<br>（手数料額、納付方法：　　） |
| ④個人情報ファイル簿の公表 | [　行っていない　]　　＜選択肢＞<br>1) 行っている　　2) 行っていない |
| 個人情報ファイル名 | |
| 公表場所 | |
| ⑤法令による特別の手続 | 特になし |
| ⑥個人情報ファイル簿への不記載等 | 特になし |
| **2. 特定個人情報ファイルの取扱いに関する問合せ** | |
| ①連絡先 | 堺市　健康福祉局　長寿社会部　医療年金課<br>〒590-0078　堺市堺区南瓦町3番1号　072-228-7375 |
| ②対応方法 | 問い合わせの受付時に受付票を起票し、対応について記録を残す。 |

# Ⅵ　評価実施手続

| 1. 基礎項目評価 | |
|---|---|
| ①実施日 | 令和4年1月31日 |
| ②しきい値判断結果 | [　　基礎項目評価及び全項目評価の実施が義務付けられる　　]<br>＜選択肢＞<br>1) 基礎項目評価及び全項目評価の実施が義務付けられる<br>2) 基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施）<br>3) 基礎項目評価の実施が義務付けられる（任意に全項目評価を実施）<br>4) 特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施） |
| **2. 国民・住民等からの意見の聴取** | |
| ①方法 | 堺市パブリックコメント制度要綱に基づき、パブリックコメントによる意見聴取を実施する。パブリックコメントの実施に際しては、広報紙に公表している旨の記事を掲載し、市ホームページ及び市内公共施設にて全文を閲覧できるようにする。 |
| ②実施日・期間 | 令和3年11月2日から令和3年12月1日まで |
| ③期間を短縮する特段の理由 | ― |
| ④主な意見の内容 | 意見なし |
| ⑤評価書への反映 | 意見なし |
| **3. 第三者点検** | |
| ①実施日 | 令和3年12月10日・令和4年1月21日 |
| ②方法 | 堺市個人情報保護審議会による第三者点検を実施した。 |
| ③結果 | 特定個人情報保護評価指針に定める目的に照らし、記載内容は妥当であると認められた。 |
| **4. 個人情報保護委員会の承認 【行政機関等のみ】** | |
| ①提出日 | |
| ②個人情報保護委員会による審査 | |

## （別添3）変更箇所

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅰ　2　システム2　② | 1～6まで記載有り | 7．持ち出し制限機能<br>：使用できる媒体を制限するとともに端末からデータを持ち出す際は上長の承認を必須とする機能。<br><br>8．生体認証機能<br>：Windowsログイン認証前に生体（顔）による認証を行う機能。 | 事前 | |
| 平成28年10月12日 | Ⅰ　7　②所属長 | 高寄　直人 | 米村　かおる | 事後 | |
| 平成28年10月12日 | Ⅱ　2　⑤保有開始日 | 平成28年1月予定 | 未定 | 事前 | |
| 平成28年10月12日 | Ⅱ　5　移転先1 | なし | 戸籍住民課への移転について記載 | 事後 | |
| 平成28年10月12日 | Ⅲ　3　リスク2　ユーザ認証の管理 | ユーザ認証は2段階で実施している。業務システムを利用するときは、まず端末のログイン時に共通基盤システムのディレクトリサービス機能において、許可された個人ごとに付与したユーザIDとパスワードにより、個人ごとのWindowsログイン認証を行っている。次に、ログインした端末から業務システムを利用する際、ユーザIDとパスワードによる認証を行っている。 | ユーザ認証は3段階で実施している。業務システムを利用するときは、まずWindowsログイン認証前に生体（顔）による認証を行い、次に共通基盤システムのディレクトリサービス機能において、許可された個人ごとに付与したユーザIDとパスワードにより、個人ごとのWindowsログイン認証を行う二要素認証を実施している。次に、ログインした端末から業務システムを利用する際は、Windowsログインのユーザ IDを利用したシングルサインオンを実施している。 | 事前 | |
| 平成28年10月12日 | Ⅲ　3　リスク2　ユーザ認証の管理 | なし | 共通基盤システムのWindowsログイン認証前に生体（顔）による認証を行うことにより、なりすましが行われないよう講じている。 | 事前 | |
| 平成28年10月12日 | Ⅲ　3　リスク4　特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置 | なし | ・許可のない外部記録媒体が使用できないように制限している。<br>・ファイルの持ち出しについて、持出し申請者を限定するとともに、上長の承認が必要であり、また、上長の承認を得たファイルは、申請した者しか持ち出すことが出来ないように制限している。<br>・いつ、誰が、どの端末で、どのデバイスに、どのファイルを持ち出し、持ち込みしたか、誰が持出し承認したかを記録するとともに、記録を取得していることを関係者に周知し、不正な持出しを抑止している。 | 事前 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
| --- | --- | --- | --- | --- | --- |
| 平成28年10月12日 | Ⅲ　5　リスク2 | ・移転を行う情報をあらかじめ仕様にて取り決め、住民情報の変更データ等を随時自動で提供する仕組みを構築している。仕様で定めた以外の情報の抜き取りを各システムから行うことは不可能で、共通基盤システムへの提供ログはシステム内に自動で保管されている。<br>・随時でデータの移転を行う際は、対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ、詳細を記録している。媒体にて他課に移転する際は、パスワードの付与を行い、第三者への漏洩を防止している。<br>・連携手段として情報連携の記録が逐一保存され、不適切な方法による特定個人情報の提供を防止している。 | ・移転を行う情報をあらかじめ仕様にて取り決め、住民情報の変更データ等を随時自動で提供する仕組みを構築している。仕様で定めた以外の情報の抜き取りを各システムから行うことは不可能で、共通基盤システムへの提供ログはシステム内に自動で保管されている。<br>・随時でデータの移転を行う際は、対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ、詳細を記録している。媒体にて他課に移転する際は、パスワードの付与を行い、第三者への漏洩を防止している。<br>・連携手段として情報連携の記録が逐一保存され、不適切な方法による特定個人情報の提供を防止している。<br>・許可のない外部記録媒体が使用できないように制限している。<br>・ファイルの持ち出しについて、持出し申請者を限定するとともに、上長の承認が必要であり、また、上長の承認を得たファイルは、申請した者しか持ち出すことが出来ないように制限している。<br>・いつ、誰が、どの端末で、どのデバイスに、どのファイルを持ち出し、持ち込みしたか、誰が持出し承認したかを記録するとともに、記録を取得していることを関係者に周知し、不正な持出しを抑止している。 | 事前 | |
| 平成28年10月12日 | Ⅲ　7　リスク1　⑨　過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか。 | 発生なし | 発生あり | 事後 | |
| 平成28年10月12日 | Ⅲ　7　リスク1　⑨　その内容 | なし | 元本市職員が、無断で持ち帰っていた選挙データや業務ファイル等を個人で契約していた民間レンタルサーバーの更改されている部分に保存した。このことにより、平成27年4月から6月までの間、インターネット上で閲覧可能な状態となり、約68万人分の有権者データなどの個人情報を流出させたもの。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅲ　7　リスク1　⑨　具体的な対策の内容 | なし | 本事案の発生を受けて、かかる事案が再び起こることのないよう、「データの外部持出し制限の強化」「情報セキュリティ等のチェック体制の強化」「事故発生時の対応強化」を柱に、ハード・ソフトの両面から再発防止の取組みを行っていく。<br><br>以下、省略 | 事後 | |
| 平成28年10月12日 | Ⅵ　1　① | 平成27年8月19日 | 平成28年4月1日 | 事後 | |
| 平成28年10月12日 | Ⅱ　4　委託の有無 | 2件 | 3件 | 事前 | |
| 平成28年10月12日 | Ⅱ．4　委託事項3 | なし | 委託事項3　①～⑨について追記 | 事前 | |
| 平成28年10月12日 | Ⅱ　別添2 | 年金資格・年金請求・年金免除について記載有り | 税情報・個人情報・宛名情報について追記 | 事後 | |
| 平成28年10月12日 | Ⅲ　7　リスク1　その他の措置の内容 | なし | 関係規定の整備<br>「データの外部持出し制限の強化」と「情報セキュリティ等のチェック体制の強化」を主な内容として、関係規定（堺市個人情報の適正管理に関する要綱、堺市情報セキュリティポリシー）を改正する。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅱ．４　委託事項1　⑧ | 事前に再委託先の商号又は名称、再委託する業務の内容、再委託する理由、その他発注者が必要とする事項を記載した書面をもって申請する。 | 業務の一部を再委託する場合については、契約書により以下の条件を課している。<br>・委託先は、個人情報取扱に係る事項について委託先同様の義務を再委託先に負わせ、再委託先に対し遵守を監督すること。<br>・再委託先事業者から委託先事業者に提出される個人情報等の保護に係る誓約書の写しを本市に提出すること。<br>・再委託先従事者から再委託先事業者に提出される秘密保持に関する誓約書の写しを本市に提出すること。<br>・再委託先の業務従事者に対するセキュリティ等に関する社員教育の実績書及び計画書を本市に提出すること。<br>また再委託の許諾については本市に提出される再委託申請書を以下の観点から審査した上で、判断する。<br>―再委託先の名称、所在地、連絡先電話番号が、正確に記載されていること。<br>―再委託が、業務の一部かつ専門的な作業であること。<br>―再委託する作業内容を具体的に明記していること。<br>―全部又は大部分の再委託でないこと。 | 事後 | |
| 平成28年10月12日 | Ⅱ　５　提供・移転の有無 | 移転を行っている　0件 | 移転を行っている　1件 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅱ．６ ③ | ＜堺市における措置＞<br>堺市情報セキュリティ対策基準要綱第8条（記録媒体の管理）に規定する「(4)不要となった記録媒体については、当該媒体に含まれる情報をいかなる方法によっても復元することができないように消去等を行ったうえで、廃棄しなければならない。」及び「(5)重要な情報を記録した記録媒体の廃棄については、その重要度に応じて、日時、処理担当者及び処理内容を記録するなど適切な処理を行わなければならない。」に基づき、以下の対策を行っている。<br>・国民年金システムにおいては、年金情報を一括削除する機能を設けており、不要になった情報については、年1回のサイクルで、復元不可能な状態での削除処理を行う。 | ＜堺市における措置＞<br>堺市情報セキュリティ対策基準要綱第8条（記録媒体の管理）に規定する「(5)不要となった記録媒体を廃棄する場合は、データ管理者の許可を得なければならない。この場合において、不要となった記録媒体については、当該媒体に含まれる情報をいかなる方法によっても復元することができないように消去等を行ったうえで、廃棄しなければならない。」及び「(6)重要な情報を記録した記録媒体の廃棄については、その重要度に応じて、日時、処理担当者及び処理内容を記録するなど適切な処理を行わなければならない。」に基づき、以下の対策を行っている。<br>・国民年金システムにおいては、年金情報を一括削除する機能を設けており、不要になった情報については、データ管理者の許可のもと、年1回のサイクルで、復元不可能な状態での削除処理を行う。 | 事後 | |
| 平成28年10月12日 | Ⅲ．３ ユーザ認証の管理 | 1. ユーザの認証方法<br>堺市情報セキュリティ対策基準要綱第１３条（職員の責務）の3に規定する「(8)操作を許可された者以外に端末機若しくはサーバーの操作方法を教示し、又は端末機若しくはサーバーの操作をさせないこと。」に基づき、以下の対策を行っている。 | 1. ユーザの認証方法<br>堺市情報セキュリティ対策基準要綱第１３条（職員の責務）第3項に規定する「(9)操作を許可された者以外に端末機若しくはサーバーの操作方法を教示し、又は端末機若しくはサーバーの操作をさせないこと。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ．３ ユーザ認証の管理 | 2. なりすましが行われないための対策<br>堺市情報セキュリティ対策基準要綱第１３条（職員の責務）の3に規定する「(9)自己の保有するパスワードに関し、他に知られないよう適切な管理を行うこと。」及び「(10)自己の保有するパスワード以外のパスワードを使用して端末機及びサーバーを操作しないこと。」に基づき、以下の対策を行っている。 | 2. なりすましが行われないための対策<br>堺市情報セキュリティ対策基準要綱第１３条（職員の責務）第4項に規定する「(1) 他人に自己の保有するIDを使用させないこと。」「(2) 自己の保有するパスワードに関し、他に知られないよう適切な管理を行うこと。」「(3) パスワードは、十分な長さのもので第三者が想像しにくいものとすること。」「(4) パスワードは、定期的に変更すること。」「(5) 端末機及びサーバにパスワードを記憶させないこと。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ，３ アクセス権限の発行・失効の管理 | 堺市情報セキュリティ対策基準要綱第１７条（アクセス制御）に規定する「(1)情報システムを利用する職員等について、情報システムごとに定められた方法に従い、その登録、変更、抹消等を行うこと」に基づき、以下の対策を行っている。 | 堺市情報セキュリティ対策基準要綱第１７条（アクセス制御）第1項に規定する「(1)情報システムを利用する職員等について、情報システムごとに定められた方法に従い、その登録、変更、抹消等を行うこと」に基づき、以下の対策を行っている。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅲ，３　アクセス権限の管理 | 堺市情報セキュリティ対策基準要綱第17条（アクセス制御）に規定している「(2) 情報システムの管理に係る権限の付与は、必要最小限の者に限ることとし、厳重に管理すること。」に基づき、以下の対策を行っている。 | 堺市情報セキュリティ対策基準要綱第17条（アクセス制御）第1項に規定している「(3) 情報システムの管理に係る権限の付与は、必要最小限の者に限ることとし、厳重に管理すること。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ，３　リスクに対する措置の内容 | 2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第5項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。 | 2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第10項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ，７　⑤ | 2. 端末設置場所<br>堺市情報セキュリティ対策基準要綱第10条（端末機及びサーバーの管理）に規定する「システム利用責任者は、執務室等に職員等がいない場合における当該執務室等の施錠等の徹底、端末機、サーバー等の固定その他情報資産の盗難防止のための措置を講じなければならない。」に基づき、以下の対策を行っている。 | 2. 端末設置場所<br>堺市情報セキュリティ対策基準要綱第10条（端末機及びサーバーの管理）第1項に規定する「システム利用責任者は、執務室等に職員等がいない場合における当該執務室等の施錠等の徹底、端末機、サーバー等の固定その他情報資産の盗難防止のための措置を講じなければならない。」に基づき、以下の対策を行っている。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅲ．７ ⑥ | ○ウイルス対策<br>堺市情報セキュリティ対策基準要綱第19条（コンピュータウイルス対策）第1項に規定する「職員等は、外部から取り入れ、又は外部へ持ち出すデータ、送受信する電子メール等については、ウイルスチェック（当該データ等にウイルスが含まれているか否かを調べることをいう。）を行うなど、ウイルスのシステムへの侵入又は外部への拡散その他ウイルスによるシステム障害等の発生の防止に努めなければならない。」及び第19条（コンピュータウイルス対策）第2項に規定する「電算管理者は、常時ウイルスに関する情報収集に努め、ウイルスチェック用の定義ファイル等は常に最新のものに保たなければならない。」に基づき、以下の対策を行っている。<br>・職員等は記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している記録媒体のみを利用している。<br>・サーバー及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させている。<br>・不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を施し、常に最新の状態を保っている。 | ○不正プログラム対策<br>堺市情報セキュリティ対策基準要綱第19条（不正プログラム対策）第1項に規定する「職員等は、外部から取り入れ、又は外部へ持ち出すデータ、送受信する電子メール等については、不正プログラムチェック（当該データ等にウイルスが含まれているか否かを調べることをいう。）を行うなど、不正プログラムのシステムへの侵入又は外部への拡散その他不正プログラムによるシステム障害等の発生の防止に努めなければならない。」及び第19条（不正プログラム対策）第2項に規定する「電算管理者は、常時不正プログラムに関する情報収集に努め、不正プログラムチェック用の定義ファイル等は常に最新のものに保たなければならない。」に基づき、以下の対策を行っている。<br>・職員等は記録媒体を使う場合、不正プログラム等の感染を防止するために、市が管理している記録媒体のみを利用している。<br>・サーバー及びパソコン等の端末に、不正プログラム対策ソフトウェアを常駐させている。<br>・不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を施し、常に最新の状態を保っている。 | 事後 | |
| 平成28年10月12日 | Ⅳ．１ ② | ＜堺市における措置＞<br>堺市情報セキュリティ対策基準要綱第２４条（監査）に規定する「電算管理者は、十分な専門的知識を有する者をして情報セキュリティについての監査を定期的にさせなければならない。」に基づき、以下の対応を行っている。 | ＜堺市における措置＞<br>堺市情報セキュリティ対策基準要綱第２４条（監査）第1項に規定する「情報セキュリティ監査統括責任者は、十分な専門的知識を有する者をして情報セキュリティについての監査を定期的にさせなければならない。」に基づき、以下の対応を行っている。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成28年10月12日 | Ⅳ．２ | 2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第5項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。 | 2. 違反行為を行った職員に対する措置<br>堺市個人情報保護条例第6章（罰則）規定及び堺市情報セキュリティ対策基準要綱第15条（侵害時の対応）第10項に規定する「市長は、職員による不正なアクセス又はその結果により、データの漏洩、破壊若しくは改ざん又はこれらを原因とするシステムダウン等により業務に深刻な影響をもたらした場合は、当該職員を懲戒処分等の対象とするものとする。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ．３　特定個人情報の使用の記録 | 堺市情報セキュリティ対策基準要綱第１６条（電子計算機及びネットワークの管理）に規定する「(1)各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、不正なアクセス等に対処できるよう一定の期間保存すること。」に基づき、以下の対策を行っている。 | 堺市情報セキュリティ対策基準要綱第１６条（電子計算機及びネットワークの管理）第1項に規定する「(1)各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、不正なアクセス等に対処できるよう一定の期間保存し、及び記録の改ざん、窃取又は不正な削除の防止のために必要な措置を講ずること。」に基づき、以下の対策を行っている。 | 事後 | |
| 平成28年10月12日 | Ⅲ，７　⑥ | ○不正アクセス対策<br>堺市情報セキュリティ対策基準要綱第17条（アクセス制御）に規定する「（6）本市の外部の組織から本市のネットワーク及び情報システムにアクセスする場合は、直接本市の内部ネットワークに接続させないこと。」に基づき、以下の対策を行っている。<br>・システムは、外部のインターネットと物理的に接続していない。<br><br>堺市情報セキュリティ対策基準要綱第１８条（ネットワーク監視）に規定する「電算管理者は、セキュリティに関する事案を検知するため、情報システムについて監視等を行わなければならない。」に基づき、以下の対策を行っている。 | ○不正アクセス対策<br>堺市情報セキュリティ対策基準要綱第17条（アクセス制御）第1項に規定する「（7）本市の外部の組織から本市のネットワーク及び情報システムにアクセスする場合は、直接本市の内部ネットワークに接続させないこと。」に基づき、以下の対策を行っている。<br>・システムは、外部のインターネットと物理的に接続していない。<br><br>堺市情報セキュリティ対策基準要綱第１８条（ネットワーク及び情報システムの監視）第１項に規定する「電算管理者は、セキュリティに関する事案を検知するため、情報システムについて監視等を行わなければならない。」に基づき、以下の対策を行っている。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成29年4月1日 | Ⅰ，５　法令上の根拠 | 番号法第九条第1項　別表第一の三十一の項 | ・番号法第九条第1項　別表第一の三十一の項<br>・行政手続における特定の個人を識別するための番号の利用等に関する抱一別表第一の主務省令で定める事務を定める命令　第二十四条の二 | 事後 | |
| 平成29年4月1日 | Ⅱ，２　⑤ | 未定 | 平成29年1月1日 | 事後 | |
| 平成29年4月1日 | Ⅱ，３　⑨ | 平成28年1月1日 | 平成29年1月1日 | 事後 | |
| 平成29年4月1日 | Ⅱ，４　委託事項2　⑥ | 株式会社アイ・オー・プロセス | シティコンピュータ株式会社 | 事後 | |
| 平成30年4月1日 | Ⅱ，２　基本情報　④記録される項目　すべての記録項目 | なし | 納付申出 | 事後 | |
| 平成30年4月1日 | Ⅱ，４　委託事項2　⑥ | シティコンピュータ株式会社 | 株式会社エス・ピー・シー | 事後 | |
| 平成30年4月1日 | Ⅵ　１　① | 平成29年4月13日 | 平成30年4月1日 | 事後 | |
| 平成30年8月27日 | Ⅰ　７　② 所属長 | 米村　かおる | 医療年金課長 | 事後 | 様式変更に伴う所要の変更 |
| 平成31年4月1日 | Ⅲ　７　⑨　その内容 | 元本市職員が、無断で持ち帰っていた選挙データや業務ファイル等を個人で契約していた民間レンタルサーバーの公開されている部分に保存した。このことにより、平成27年4月から6月までの間、インターネット上で閲覧可能な状態となり、約68万人分の有権者データなどの個人情報を流出させたもの。 | 平成29年4月10日（月）から運用を開始した電子メールの誤送信防止システムにおいて、「BCC」に記入されたメールアドレスを誤って「TO」に自動的に変換するよう設定していた。<br>そのため、4通の電子メールが本来「BCC」に記入して送信されるところ、「TO」に変換され、受信者にすべてのメールアドレスが表示される形で送信された。結果、219件のメールアドレスを流出させたもの。 | 事後 | |
| 平成31年4月1日 | Ⅲ　７　⑨　再発防止策の内容 | 本事案の発生を受けて、かかる事案が再び起こることのないよう、「データの外部持出し制限の強化」「情報セキュリティ等のチェック体制の強化」「事故発生時の対応強化」を柱に、ハード・ソフトの両面から再発防止の取組みを行っていく。 | システムに求めている要件、システム設定内容及びテスト結果の確認を徹底する。 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
| --- | --- | --- | --- | --- | --- |
| 平成31年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | （1）データの外部持出し制限の強化<br>ア　外部記録媒体（USBメモリー等）の接続制限の拡充<br>　一部の業務システムで既に実施している外部記録媒体の接続制限を、他の業務システムにも拡充し、承認を受けていない外部記録媒体の接続ができないようにする。<br>イ　データの外部持出し承認の厳格化<br>　承認を受けた外部記録媒体であっても、データの外部保存を行う場合は、システム上での本人の認証に加え、所属長による承認を必要とすることとし、承認がなければ外部記録媒体へのデータ記録ができないようにする。<br>ウ　データの外部持出し操作記録（ログ）取得の拡充<br>　一部の業務システムで既に実施しているデータの外部持出しの操作記録（ログ）の取得を、他の業務システムにも拡充し、データの外部持出しを行った場合、詳細な記録が残るようにする。<br>エ　電子メールの誤送信を防ぐ措置の実施<br>　電子メールの誤送信による個人情報の流出を防止するため、電子メールの送信時に一定の待機時間を設定する。また、添付ファイルを外部に送信する際の所属長による承認機能やメールのあて名を「TO」や「CC」から「BCC」へと強制的に変換する機能等を導入する。<br>オ　データのシステム外への持出し時のデータの暗号化<br>　住民情報系システムの端末から、データを外部に持ち出す場合には、強制的にパスワードを付与し、データを暗号化する仕組みを導入する。 | 同上 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
| --- | --- | --- | --- | --- | --- |
| 平成31年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | （2）情報セキュリティ等のチェック体制の強化<br>ア　副市長をトップとする指揮命令体制の構築<br>　個人情報保護と情報セキュリティについて、それぞれを統括する副市長を最高責任者とする指揮命令体制を構築し、セキュリティ体制・方策などについて検証する。<br>イ　個人情報取扱事務の届出手続きの変更<br>　職務上、個人情報を取り扱う部署の所属長（個人情報保護管理者）に対して、現在、個人情報の取扱いを開始する場合や変更する場合に届出を求めているが、これに加え、毎年度当初及び必要に応じて、個人情報の取扱状況と保護体制の確認、報告を求めるものとする。<br>ウ　情報セキュリティに関する外部監査の実施<br>　職務上、個人情報を取り扱う部署を中心に、適切な情報セキュリティが取られているかどうかを第三者により監査する「情報セキュリティ外部監査」を実施する。（平成１５年度から継続して実施中） | 同上 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成31年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | (3)事故発生時の対応の強化<br>ア　副市長をトップとする指揮命令体制の構築<br>≪再掲≫<br>　個人情報保護と情報セキュリティについて、それぞれを統括する副市長を最高責任者とする指揮命令体制を構築し、万が一の事故発生時に適切な事故対応が的確に取れるようにする。<br>イ　関係部局による事故対策会議の設置<br>　(2)アで的確な判断が下せるよう、個人情報保護、情報セキュリティ、職員の服務管理等の所管部局からなる「個人情報流出等事故対策会議」を設置し、万が一の事故発生時に速やかに情報を収集、共有、報告できるようにする。<br>ウ　外部有識者からの意見聴取(情報セキュリティアドバイザーの選任)<br>　(2)アで的確な判断が下せるよう、個人情報保護と情報セキュリティに関する有識者(弁護士、大学教授等)を「情報セキュリティアドバイザー」に選任し、万が一の事故発生時に専門的知見からの意見を聴取する。<br>エ　迅速なレスポンスチームの編成<br>　インシデント発生時には、瞬時に必要なレスポンスが取れるよう、少人数の初動体制(レスポンスチーム)を編成する。また、演習や訓練を実施し、有事の際の実効性を高める。 | 同上 | 事後 | |
| 平成31年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | (4)職員の意識向上<br>ア　職員一人ひとりが、情報セキュリティ対策の必要性と内容を十分に理解し、個人情報の適正な管理を行うことを目的として、全職員を対象に、個人情報保護と情報セキュリティに関する研修を実施し、研修の内容の理解度を図るテストを実施する。<br>イ　職員に対し情報セキュリティに関する日常の啓発を強化する。 | 同上 | 事後 | |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 平成31年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | (5)その他<br>ア　二要素認証の導入<br>　住民情報系端末システムにおいて、なりすまし利用を防止する為、Windowsへのログイン時に、従来のIDとパスワードによる認証に加え、生体等による認証を導入する。<br>イ　業務アプリ等の管理<br>　エクセルやアクセスを使った職員の自作システム(業務アプリ)の運用においては、ガイドライン等を定めて要件定義と基本設計を適切に行うとともにデータの適正管理を徹底する。 | 同上 | 事後 | |
| 平成31年4月1日 | Ⅲ　7　その他の措置の内容 | 関係規定の整備<br>「データの外部持出し制限の強化」と「情報セキュリティ等のチェック体制の強化」を主な内容として、関係規定(堺市個人情報の適正管理に関する要綱、堺市情報セキュリティポリシー)を改正する。 | 関係規定の整備<br>メール送信によるインシデント発生を防ぐため、個人情報を含む重要な情報を送信する際のメール使用の是非を慎重に判断するよう関係規定(堺市情報セキュリティポリシー)を改正した。 | 事後 | |
| 平成31年4月1日 | Ⅵ　1　①実施日 | 平成30年4月1日 | 平成31年4月1日 | 事後 | |
| 令和2年4月1日 | Ⅲ　5　リスク1　不正な提供・移転が行われるリスク　その他の措置の内容 | ・遠隔地保管を行うバックアップ用LTOメディアは、情報課推進課が一括管理しており、所属課との受渡しは記録簿にて管理を行っている。 | ・遠隔地保管を行うバックアップ用LTOメディアの運送業者への受渡しは記録簿にて管理を行っている。 | 事後 | 庁内一括管理から各課での管理変更に伴う変更 |
| 令和2年4月1日 | Ⅴ　1　①請求先 | 堺市　市長公室　広報部　市政情報課 | 堺市　市長公室　広報戦略部　市政情報課 | 事後 | 組織変更に伴う課名変更 |
| 令和2年4月1日 | Ⅵ　1　①実施日 | 平成31年4月1日 | 令和2年4月1日 | 事後 | 定期評価に伴う変更 |
| 令和3年4月1日 | Ⅰ　1　②事務の内容 | 手帳再交付申請 | 手帳(R4.4.1～基礎年金番号通知書)再交付申請 | 事後 | 制度変更に伴う文言修正 |
| 令和3年4月1日 | Ⅰ　7　①評価実施機関における担当部署 | 健康福祉局　生活福祉部　医療年金課 | 健康福祉局　長寿社会部　医療年金課 | 事後 | 組織変更に伴う課名変更 |
| 令和3年4月1日 | Ⅱ，2　⑥ | 健康福祉局　生活福祉部　医療年金課 | 健康福祉局　長寿社会部　医療年金課 | 事後 | 組織変更に伴う課名変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| 令和3年4月1日 | Ⅴ　2　①連絡先 | 堺市　健康福祉局　生活福祉部　医療年金課 | 堺市　健康福祉局　長寿社会部　医療年金課 | 事後 | 組織変更に伴う課名変更 |
| 令和3年4月1日 | Ⅲ　7　⑨　その内容 | 平成29年4月10日（月）から運用を開始した電子メールの誤送信防止システムにおいて、「BCC」に記入されたメールアドレスを誤って「TO」に自動的に変換するよう設定していた。<br>そのため、4通の電子メールが本来「BCC」に記入して送信されるところ、「TO」に変換され、受信者にすべてのメールアドレスが表示される形で送信された。結果、219件のメールアドレスを流出させたもの。 | 受託業者が、長屋建て住宅の所有者を対象とした調査を行った、アンケート調査票に所有者本人以外の氏名を誤って印字した調査票を誤送付（1,461件の個人情報が漏洩） | 事後 | 印字誤りによる流出事故に係る変更 |
| 令和3年4月1日 | Ⅲ　7　⑨　再発防止策の内容 | システムに求めている要件、システム設定内容及びテスト結果の確認を徹底する。 | ・受託業者に対し、個人情報を取り扱う場合のマニュアルやチェックリストと、十分な確認が必要な作業の場合、市からの指示に基づく手順書を作成させることにより、個人情報の適正管理、適正な事務処理について、指導と確認を徹底した。<br>・市として、再びこのような事案が発生しないよう、個人情報保護の重要性を再認識し、個人情報を取り扱う作業の場合、受託業者に対し、書面により詳細な作業手順や注意点を明確に指示し、漏洩や手順の誤りがないことの確認を徹底した。 | 事後 | 印字誤りによる流出事故に係る変更 |
| 令和3年4月1日 | Ⅴ　2　①連絡先 | 堺市　健康福祉局　生活福祉部　医療年金課 | 堺市　健康福祉局　長寿社会部　医療年金課 | 事後 | 組織変更に伴う課名変更 |
| 令和3年4月1日 | Ⅵ　1　①実施日 | 令和2年4月1日 | 令和3年4月1日 | 事後 | 定期評価に伴う変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| | Ⅰ　2　システム2　③他のシステムとの接続 | 略 | [〇]　庁内連携システム | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅰ　2　システム4 | なし | システム4を追記 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅰ | なし | （別添1）事務内容（標準化後）を追加 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅱ　3　⑦使用の主体　使用部署 | 健康福祉局　生活福祉部　医療年金課　及び各区保険年金課 | 健康福祉局　長寿社会部　医療年金課　及び各区保険年金課 | 事後 | 組織変更に伴う課名変更 |
| | Ⅱ　4　委託事項1 | システムの運用保守業務 | システムの運用保守業務及び標準準拠システムへの移行に伴うデータ抽出業務並びに標準準拠システム構築業務 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅱ　4　委託事項1　①委託の内容 | システムの運用保守業務を行うにあたり、必要な範囲で特定個人情報ファイルの取扱いを委託 | システムの運用保守業務及び標準準拠システムへの移行に伴うデータ抽出業務並びに標準準拠システムを構築する業務を行うにあたり、必要な範囲で特定個人情報ファイルの取扱いを委託 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅱ　4　委託事項1　④委託先への特定個人情報ファイルの提供方法 | その他（堺市役所庁舎設置のサーバー内又は端末機内での提供） | その他（堺市役所庁舎設置のサーバー内又は端末機内及びガバメントクラウド内での提供） | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| | Ⅱ　６　①保管場所 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。<br>・ISO/IEC27017、ISO/IEC27018の認証を受けていること。<br>・日本国内でのデータ保管を条件としていること。<br>②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅱ　６　③消去方法 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>①特定個人情報の消去は本市からの操作によって実施される。本市の業務データは国及びガバメントクラウドのクラウド事業者にはアクセス制御されているため特定個人情報を消去することはない。<br>②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、ISO/IEC27002等にしたがって確実にデータ消去する。<br>③既存システムについては、本市が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅲ　３　アクセス権限の発行・失効の管理　具体的な管理方法 | 情報化推進課 | ICTイノベーション推進室 | 事後 | 組織変更に伴う課名変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| | Ⅲ　5　リスク1　不正な提供・移転が行われるリスク　特定個人情報の提供・移転の記録　具体的な方法 | 情報化推進課 | ICTイノベーション推進室 | 事後 | 組織変更に伴う課名変更 |
| | Ⅲ　7　リスク1　⑤物理的対策<br>　具体的な対策の内容 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>1．ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。<br><br>2．事前に許可されていない装置等に関しては、外部に持出できないこととしている。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅲ　7　リスク1　⑥技術的対策<br>具体的な対策の内容 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>1．国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。<br><br>2．地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。<br><br>3．クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| | 同上（上の続き） | 同上（上の続き） | （上の続き）<br>4・クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。<br><br>5・地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。<br><br>6. ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。<br><br>7. 地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。<br><br>8. 地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅲ　7　リスク3　消去手順<br>手順の内容 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |
| | Ⅳ　1　②監査<br>具体的な内容 | 略 | 略<br>＜ガバメントクラウドにおける措置＞<br>ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 | 事前 | ガバメントクラウドへのシステム移行に伴う変更 |

| 変更日 | 項目 | 変更前の記載 | 変更後の記載 | 提出時期 | 提出時期に係る説明 |
|---|---|---|---|---|---|
| | Ⅳ　3.その他のリスク対策 | なし | ＜ガバメントクラウドにおける措置＞<br>ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。 | 事前 | ガバメントクラウドへの移行に伴う変更 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |