特定個人情報保護評価書（全項目評価書）

※ 4.0.3版からの修正個所は 赤枠 で囲ってあります。

（過去３年以内の個人情報に関する重大事故の更新、
「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ついて」の記載更新）

評価書番号	評価書名

※ 空欄のほか、情報連携基盤システム・中間サーバーに関して記入済みの欄についても評価対象事務に関して記入してください。

※ ぴったりサービス（サービス検索・電子申請機能）を利用する場合の記載を 緑枠 で囲ってあります。

※ 評価書の作成にあたっては、本記載例のほか、個人情報保護委員会が提供する以下の資料を確認してください。
- 『特定個人情報保護評価指針』
- 『特定個人情報保護評価指針の解説』
- 評価書の記載要領
- 『特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）』 等

個人のプライバシー等の権利利益の保護の宣言	
特記事項	

※評価対象事務での措置の内容を記載する場合において、具体的な措置の内容が記載できる場合は記載してください。

※ガバメントクラウド上の情報連携基盤システムは令和6年10月以降に稼働の予定です。
令和8年3月末（予定）までは現行の情報連携基盤システムと並行稼働するので、評価対象事務でガバメントクラウド上の情報連携基盤システムの利用を開始する時期にあわせて修正してください。
関係する記載を 青枠 で囲ってあります。

※情報連携基盤システムシステムの共通標準化基準への対応は令和6年度の予定です。
評価対象事務で団体内統合宛名番号での連携から住民番号及び住登外者宛名番号に連携方法を変更する時期に合わせて評価の再実施をしてください。
関係する記載を 水色枠 で囲ってあります。

評価実施機関名

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	
②事務の内容　※	
③対象人数	[　　] ＜選択肢＞ 1) 1,000人未満　　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　　4) 10万人以上30万人未満 5) 30万人以上

「〇〇に関する事務」とし、評価書名と一致させること。

ぴったりサービス（サービス検索・電子申請機能）を利用する場合、現行の窓口や郵送での書類の受け入れ以外に、ぴったりサービス（サービス検索・電子申請機能）での受領を追記すること。

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	〇〇システム
②システムの機能	
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　　[〇]庁内連携システム [　]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 [〇]宛名システム等　　[　]税務システム [〇]その他　（ 申請管理システム　　）

業務システムの名称を記載すること。

情報連携基盤システムと接続する場合には、「庁内連携システム」、「宛名システム等」及び「その他（申請管理システム）」を選択すること。
情報提供ネットワークシステム及び中間サーバーには直接接続しないため、選択しないこと。
既存の業務システムとの直接連携はなくす方針のため、「既存住民基本台帳システム」や「税務システム」は選択しないこと。ただし、個人番号保有日以降も他の業務システムと直接情報連携する場合にはそのシステムの正式名称を記入し、情報連携基盤システム対応後に修正すること。

システム2～5	
システム2	
①システムの名称	情報連携基盤システム（庁内連携システム、宛名システム等及び申請管理システム）
②システムの機能	(1) 宛名番号付番機能 団体内統合宛名番号が未登録の個人について、新規に団体内統合宛名番号を付番する機能。既存業務システムからの団体内統合宛名番号要求に対し、団体内統合宛名番号を付番し既存業務システム及び中間サーバーに対し返却する。 (2)住登外者宛名番号管理機能 既存業務システムからの住登外者宛名番号の紐付情報を保存し、管理する機能。既存システム連携時には各既存業務システムの住登外者宛名番号を置換する。 (3) 宛名情報等管理機能 宛名情報を団体内統合宛名番号、個人番号と紐付けて保存し、管理する機能。 (4) 中間サーバー連携機能 中間サーバーまたは中間サーバー端末からの要求に基づき、団体内統合宛名番号に紐付く宛名情報等を通知する機能。 (5) 既存システム連携機能 既存業務システムからの要求に基づき、宛名番号、個人番号、団体内統合宛名番号又は受付番号に紐付く宛名情報等を通知する機能。 (6) セキュリティ管理機能 暗号化機能及び情報照会・提供記録等を管理する機能。 (7) 職員認証・権限管理機能 情報連携基盤システムを利用する職員または業務システムの認証と付与された権限に基づいた各種機能や宛名情報へのアクセス制御を行う機能。 (8) システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能。 (9)ぴったりサービス連携機能 ぴったりサービス（サービス検索・電子申請機能）で受け付けた電子申請データを申請管理システムに連携する（受け渡す）機能。 (10)申請管理システム 連携サーバーから連携された電子申請データを参照する機能。 (11)電子証明書シリアル番号変換機能 連携サーバーから連携された電子申請データに含まれるマイナンバーカードの電子証明書のシリアル番号と宛名番号を紐付ける機能。 (12)申請状況確認機能 ぴったりサービスから受信した申請情報及び処理状況等を確認する機能。
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 [　　] 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 [　　] 宛名システム等　　[○] 税務システム [○] その他　（ 中間サーバー、情報連携基盤システムを利用する業務システム、ぴったりサービス（サービス検索・電子申請機能） ）

評価対象事務で、情報連携基盤システム（情報照会・提供）を利用する場合には、このとおり記載すること。

システム3	
①システムの名称	中間サーバー
②システムの機能	(1) 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 (2) 情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う機能。 (3) 情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能。 (4) 既存システム接続機能 中間サーバーと既存業務システム、宛名システム及び既存住民基本台帳システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能。 (5) 情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する機能。 (6) 情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する機能。 (7) データ送受信機能 中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 (8) セキュリティ管理機能 暗号化／復号機能と、鍵情報及び照会許可用照合リスト情報を管理する機能。 (9) 職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能。 (10)システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能。
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 [　]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 [○]宛名システム等　[　]税務システム [　]その他　(　　)

システム4	
①システムの名称	ぴったりサービス(サービス検索・電子申請機能)
②システムの機能	【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能
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 [　]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 [○]宛名システム等　[　]税務システム [　]その他　(　　)
システム6～10	
システム11～15	
システム16～20	

評価対象事務で、中間サーバーを利用する場合（情報提供ネットワークシステムを利用した情報照会、情報連携基盤システムを通じた中間サーバーへの情報提供を含む。）には、このとおり記載すること。

評価対象事務で、ぴったりサービス（サービス検索・電子申請機能）利用時に個人番号を取得する場合には、このとおり記載すること。
※個人番号を取得しない場合は記載不要。

住民記録システム、住民基本台帳ネットワークシステム等、その他にも評価対象事務で利用するシステムがあれば記載すること。
個人番号保有日以降も住民記録システム連携サーバーや他の業務システムと直接情報連携する場合にはそのシステムについて記載が必要となり、情報連携基盤システムを利用した情報連携に対応する時点で修正すること。
評価実施部署とシステム所管部署が異なる場合には、システム所管部署に評価書に記載すべき内容を確認すること。

3. 特定個人情報ファイル名	
1. 宛名ファイル 2. ○○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	
②実現が期待されるメリット	
5. 個人番号の利用　※	
法令上の根拠	
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	[　　] <選択肢> 1) 実施する 2) 実施しない 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	
②所属長の役職名	
8. 他の評価実施機関	

情報連携基盤システム、中間サーバーを利用する場合には「宛名ファイル」として、個人番号と宛名番号及び住登外者宛名番号を紐付ける特定個人情報ファイルを含めること。
（評価対象事務の他の特定個人情報ファイル（○○ファイル）に宛名ファイルに該当する項目を含めても可）

別表に記載された個人番号利用事務については、別表の項の番号を記載すること。

個人番号の独自利用及び同一機関内における特定個人情報ファイルの移転がある場合（別表記載の事務を含む。）には、「番号利用法第9条第2項」及び「名古屋市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施行条例」（番号利用条例）を記載すること。

番号利用法第19条第8項に基づく主務省令第2条の表の項の番号を記載すること。

評価対象事務に個人番号の独自利用事務を含み、情報提供ネットワークによる情報連携を行う場合には次の事項を記載すること。
・番号利用法第19条第17号
・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第十九条第八号に基づく特定個人情報の提供に関する規則
・名古屋市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施行条例

（別添1）事務の内容
（備考）

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		
1. 宛名ファイル		
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＞ 1）システム用ファイル 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		[　100万人以上1,000万人未満　] ＜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
③対象となる本人の範囲 ※		(1) 区域内の住民（住基法第5条（住民基本台帳の備付け）に基づき住民基本台帳に記録された住民を指す） ※住民基本台帳に記録されていた者で、転出・死亡等の事由により住民票が消除された者を含む。 (2) 区域外の住民で、情報連携基盤システムを利用する個人番号利用事務で対象となる者 (3) 区域外の住民で、情報連携基盤システムを利用する個人番号利用事務以外の事務で対象となる者
	その必要性	情報提供ネットワークシステムによる情報照会・提供及び情報連携基盤システムを利用した団体内の情報連携にあたり、団体内で個人を一意に識別する必要があるため。 また、マイナポータルで入力された申請情報に含まれるマイナンバーカードの電子証明書のシリアル番号と宛名番号を紐付ける必要があるため。
④記録される項目		[　　10項目未満　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 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 [○] 個人番号　[○] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [　] 4情報（氏名、性別、生年月日、住所）　[　] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[　] 地方税関係情報　[　] 健康・医療関係情報 [　] 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 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [　] その他　（　　）
	その妥当性	宛名ファイルがないと、団体内で各業務システムが管理する個人を一意に識別できず、情報提供ネットワークシステムによる情報照会・提供及び情報連携基盤システムを利用した団体内の情報連携ができない。 また、宛名ファイルがないと、マイナポータルで入力された申請者を団体内で一意に識別できず、申請情報に含まれる4情報（氏名、性別、生年月日、住所）による申請者の特定が必要となる。 なお、「③対象となる本人の範囲」の(3)については、個人番号及び個人番号対応符号は記録項目に含まない。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成〇年〇月〇日
⑥事務担当部署		〇〇局〇〇部〇〇課、総務局行政DX推進部デジタル改革推進課

情報連携基盤システム及び中間サーバーで保有する宛名ファイルを利用する場合にはこのとおり記載すること。
（評価対象事務の他の特定個人情報ファイル（〇〇ファイル）に宛名ファイルに該当する項目を含める場合には、「宛名ファイル」と「〇〇ファイル」の記載内容を統合すること）

宛名ファイルの事務担当部署には、業務システム所管課（または事務の所管課）及びデジタル改革推進課を記載すること。

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 [○] 評価実施機関内の他部署 （ スポーツ市民局地域振興部住民課（既存住民基本台帳システム） ） [○] 行政機関・独立行政法人等 （ 地方公共団体情報システム機構 ） [ ] 地方公共団体・地方独立行政法人 （ ） [ ] 民間事業者 （ ） [ ] 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 [ ] 電子メール [ ] 専用線 [ ] 庁内連携システム [○] 情報提供ネットワークシステム [○] その他 （ 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 ）
③入手の時期・頻度		住民については、住民基本台帳が更新される都度、随時入手する。
④入手に係る妥当性		
⑤本人への明示		
⑥使用目的 ※		
	変更の妥当性	-
⑦使用の主体	使用部署 ※	
	使用者数	[ ] ＜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
⑧使用方法 ※		＜情報連携基盤システム・中間サーバー＞ 団体内統合宛名番号で団体内で個人を一意に識別することにより、情報提供ネットワークシステムによる情報照会・提供及び情報連携基盤システムを利用した団体内の情報連携に対応する。また、住民番号及び住登外者宛名番号で情報連携基盤システムを利用した団体内の情報連携に対応する。 ＜情報連携基盤システム＞ ぴったりサービス（サービス検索・電子申請機能）を通じて申請された電子申請データの受理、審査等。
	情報の突合 ※	＜情報連携基盤システム・中間サーバー＞ 同一個人の重複登録が行われないように、新規登録の際に登録済みの者との突合を行う。 ＜情報連携基盤システム＞ 申請者を確認するために既存住基システムを通じて取り込んだ番号紐付情報と突合する。
	情報の統計分析 ※	＜情報連携基盤システム・中間サーバー＞ 実施しない。
	権利利益に影響を与え得る決定 ※	＜情報連携基盤システム・中間サーバー＞ 該当なし。
⑨使用開始日		

入手元は、評価対象事務に応じて選択すること。
評価実施機関内の他部署（スポーツ市民局地域振興部住民課）…市長部局で住基情報を利用する場合
行政機関・独立行政法人等（地方公共団体情報システム機構）…住基ネットの機構保有本人確認情報を利用する場合
その他（スポーツ市民局地域振興部住民課）…市長以外の機関で住基情報を利用する場合

入手方法は、評価対象事務に応じて選択すること。
情報提供ネットワークシステム…符号の取得に利用するもので、情報提供ネットワークシステムを利用した情報照会や中間サーバーへの情報提供を行う場合
その他（住基ネット）…住基ネットの機構保有本人確認情報を利用する場合
その他（既存住基システム）…住基情報を利用する場合

評価対象事務でその他の方法でも入手する場合には（住民以外の者の特定個人情報を入手する場合や本人から個別に入手する場合等）には、その時期や頻度についても記載すること。

評価対象事務での使用方法も記載すること。

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> 1）委託する 2）委託しない （ 1 ）件
委託事項1		情報連携基盤システムの開発委託、運用保守委託
①委託内容		情報連携基盤システムの開発、運用保守
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> 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	[100万人以上1,000万人未満] <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 ※	2. ③対象となる本人の範囲と同じ
	その妥当性	システムの開発・運用保守を実施するために、特定個人情報ファイル全体を委託の対象にする必要がある。
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。） [ ]フラッシュメモリ [ ]紙 [○]その他 （ 情報連携基盤システムを設置する情報管理室内でのシステムの直接操作 ）
⑤委託先名の確認方法		名古屋市契約事務手続要綱に基づく入札結果等の公表、名古屋市電子調達システムでの随意契約内容の公表、名古屋市情報公開条例に基づく公開請求により確認することができる。
⑥委託先名		日本電気株式会社 東海支社
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	再委託先名称、再委託先の業務範囲、業務期間、業務従事者名簿、再委託の理由、再委託先の選定理由、再委託先に取得情報の取扱いに関して委託先に課せられている事項と同一の事項を遵守させる旨が記載された申請書の提出を受け、承諾を判断する。
	⑨再委託事項	情報連携基盤システムの開発、運用保守に関する業務の一部（プロジェクトマネージャー及び運用管理責任者に関する業務は除く。）
委託事項2～5		
委託事項6～10		
委託事項11～15		
委託事項16～20		

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　（　　）件　[　]移転を行っている　（　　）件 [○]行っていない
提供先1	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[　　] <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
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[　]情報提供ネットワークシステム　[　]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。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑦時期・頻度	
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] <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
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[　]庁内連携システム　[　]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。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

宛名ファイルは個人番号利用事務では提供・移転の対象ではないため「行っていない」を選択する。

6. 特定個人情報の保管・消去

①保管場所 ※		＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムは、ガバメントクラウド及び庁舎内の情報管理室に設置し、情報管理室への入退室を厳重に管理する。 ②特定個人情報は、ガバメントクラウド及び情報管理室内に設置された機器に保存する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ガバメントクラウドにおける措置＞ 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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 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	［　定められていない　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	団体内統合宛名番号に紐付く全ての特定個人情報が不要となるまで保管する必要があるため、宛名ファイルとしての期間を定めることができない。
③消去方法		＜情報連携基盤システムにおける措置＞ ①団体内統合宛名番号に紐付く特定個人情報の情報連携が不要になった時点で削除する。 ②情報管理室に設置された機器のディスク交換やハード更改等の際は、情報連携基盤システム運用機器の保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。消去を行ったときは、電子情報を復元不可能な方法によって消去したことを証する写真その他の証拠を添えた証明書等を提出して、委託者の確認を受ける。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体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が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。 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、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体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

評価対象事務に係る各システムにおいて実際に付している証明があれば具体的に記載する。

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		
2. ○○ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　] ＜選択肢＞ 1）システム用ファイル 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		[　　] ＜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
③対象となる本人の範囲 ※		
	その必要性	
④記録される項目		[　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 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 [　]個人番号　[　]個人番号対応符号　[　]その他識別情報（内部番号） ・連絡先等情報 [　]4情報（氏名、性別、生年月日、住所）　[　]連絡先（電話番号等） [　]その他住民票関係情報 ・業務関係情報 [　]国税関係情報　[　]地方税関係情報　[　]健康・医療関係情報 [　]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 [　]生活保護・社会福祉関係情報　[　]介護・高齢者福祉関係情報 [　]雇用・労働関係情報　[　]年金関係情報　[　]学校・教育関係情報 [　]災害関係情報 [　]その他　（　　）
	その妥当性	
	全ての記録項目	別添2を参照。
⑤保有開始日		平成○年○月○日（ただし、「（別添2）ファイル記録項目」で●印をつけた記録項目は、番号利用法第9条第2項の規定に基づく番号利用条例の関連規程を根拠に同一機関内の他の部署から移転される特定個人情報であるため、当該条例の関連規程が制定された場合に保有する予定である。）
⑥事務担当部署		

宛名ファイル以外の特定個人情報ファイルについて記載すること。

庁内連携に関する番号利用条例を根拠に他の個人番号利用事務又は個人番号関係事務から移転する特定個人情報ファイルの場合には、番号利用条例の関連規程が未制定のため保有しないが、関連規程が制定された場合に保有する予定である旨を記載すること。
番号利用法第9条第1項の利用の範囲内となる特定個人情報と庁内連携に関する番号利用条例を根拠に移転される特定個人情報を同一の特定個人情報ファイルにまとめている場合には、[7.備考]又は「（別添2）ファイル記録項目」欄で番号利用条例の関連規程が制定された場合に保有する予定となる特定個人情報の範囲（記録項目等）を明記すること。

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 [　]評価実施機関内の他部署　（　　） [　]行政機関・独立行政法人等　（　　） [　]地方公共団体・地方独立行政法人　（　　） [　]民間事業者　（　　） [　]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 [　]電子メール　[　]専用線　[　]庁内連携システム [　]情報提供ネットワークシステム [　]その他　（　　）
③入手の時期・頻度		
④入手に係る妥当性		
⑤本人への明示		
⑥使用目的 ※		
	変更の妥当性	
⑦使用の主体	使用部署 ※	
	使用者数	[　]　＜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
⑧使用方法 ※		
	情報の突合 ※	
	情報の統計分析 ※	
	権利利益に影響を与え得る決定 ※	
⑨使用開始日		

庁内の情報連携については、業務システムの直接連携や外部記録媒体ではなく、情報連携基盤システムを利用する方針である。
電子記録媒体、フラッシュメモリ…庁内の情報連携では使用しない
庁内連携システム…情報連携基盤システムを使用する場合
情報提供ネットワークシステム…番号利用法別表第2、番号利用法第19条第9号に基づく個人情報保護委員会規則により、情報提供ネットワークシステムから取得する場合
その他…情報連携基盤システム導入に伴い、業務システムとの直接連携は行わないため、業務システムは記載しない（ただし、個人番号保有日以降も他の業務システムと直接情報連携する場合にはそのシステムの正式名称を記入し、情報連携基盤システム対応後に修正すること。）。また、ぴったりサービス（サービス検索・電子申請機能）を利用する場合はぴったりサービス（サービス検索・電子申請機能）及び申請管理システムを記載する。

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> 1）委託する　　2）委託しない （　　）件
委託事項1		情報連携基盤システムの開発委託、運用保守委託
①委託内容		情報連携基盤システムの開発、運用保守
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	[　　]　　<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 ※	
	その妥当性	システムの開発・運用保守を実施するために、情報連携基盤システムに提供する特定個人情報ファイルを委託の対象にする必要がある。
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。） [　]フラッシュメモリ　　[　]紙 [○]その他　（ 情報連携基盤システムを設置する情報管理室内でのシステムの直接操作　）
⑤委託先名の確認方法		名古屋市契約事務手続要綱に基づく入札結果等の公表、随意契約内容の公表、名古屋市情報公開条例に基づく公開請求により確認することができる。
⑥委託先名		日本電気株式会社　東海支社
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	再委託先名称、再委託先の業務範囲、業務期間、業務従事者名簿、再委託の理由、再委託先の選定理由、再委託先に取得情報の取扱いに関して委託先に課せられている事項と同一の事項を遵守させる旨が記載された申請書の提出を受け、承諾を判断する。
	⑨再委託事項	情報連携基盤システムの開発、運用保守に関する業務の一部（プロジェクトマネージャー及び運用管理責任者に関する業務は除く。）

委託事項2～5		
委託事項2		
①委託内容		
②取扱いを委託する特定個人情報ファイルの範囲		[　　] ＜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	[　　] ＜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　※	
	その妥当性	
③委託先における取扱者数		[　　] ＜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。） [　]フラッシュメモリ　[　]紙 [　]その他　（　　）
⑤委託先名の確認方法		
⑥委託先名		
再委託	⑦再委託の有無　※	[　　] ＜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6～10		
委託事項11～15		
委託事項16～20		

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 （ ）件 [○] 移転を行っている （ ）件 [ ] 行っていない
提供先1	
①法令上の根拠	番号利用法第19条第8号に基づく主務省令第2条の表 ○項
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[ ] ＜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
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 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。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
提供先2～5	
提供先2	
①法令上の根拠	
②提供先における用途	
③提供する情報	
④提供する情報の対象となる本人の数	[ ] ＜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
⑤提供する情報の対象となる本人の範囲	
⑥提供方法	[ ] 情報提供ネットワークシステム [ ] 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。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	
①法令上の根拠	名古屋市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施行条例(案)
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[　　] <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
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[○]庁内連携システム　　[　]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。) [　]フラッシュメモリ　　[　]紙 [　]その他　（　　）
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

庁内連携に関する番号利用条例を根拠に他の個人番号利用事務に移転する場合には、
関係規程が未制定であることがわかるように条例名に（案）を記載すること。

6. 特定個人情報の保管・消去

①保管場所 ※		＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムは、ガバメントクラウド及び庁舎内の情報管理室に設置し、情報管理室への入退室を厳重に管理する。 ②特定個人情報は、ガバメントクラウド及び情報管理室内に設置された機器に保存する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①システム内のデータは、セキュリティゲートにて入退館管理をしている建物のうち、さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。 ②外部記録媒体は、施錠できるキャビネットに保管している。 ＜ガバメントクラウドにおける措置＞ 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。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 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	[　　] ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	
③消去方法		＜〇〇システムにおける措置＞ ①… ②移転・提供が不要となった特定個人情報について、定期的に情報連携基盤システム上から削除する。 ＜情報連携基盤システムにおける措置＞ ①保管期間を過ぎた特定個人情報は定期的に削除する。 ②情報管理室に設置された機器のディスク交換やハード更改等の際は、情報連携基盤システム運用機器の保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。消去を行ったときは、電子情報を復元不可能な方法によって消去したことを証する写真その他の証拠を添えた証明書等を提出して、委託者の確認を受ける。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。 ＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①LGWAN 接続端末に一時的に記録した個人番号付電子申請データは、紙に打出し後、速やかに完全消去する。 ②外部記録媒体に一時的に記録した個人番号付電子申請データは、使用の都度速やかに完全消去する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体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が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。 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、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体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

評価対象事務に係る各システムにおいて実際に付している証明があれば具体的に記載する

（別添2）特定個人情報ファイル記録項目

1．宛名ファイル
(1)個人番号、(2)個人番号対応符号、(3)団体内統合宛名番号、(4)住民番号（既存住民基本台帳システムの宛名番号）、(5)住登外者宛名番号、(6)情報照会提供記録、(7)アクセスログ、(8)シリアル番号

2．〇〇ファイル
(1)受付番号、(2)

ぴったりサービス（サービス検索・電子申請機能）より申請情報を取得する場合には、
「宛名ファイル」の記録項目にシリアル番号、「〇〇ファイル」の記録項目に受付番号を含めること。

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	
1. 宛名ファイル	
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	
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	
その他の措置の内容	
リスクへの対策は十分か	[　　] ＜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： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	＜情報連携基盤システム・中間サーバーにおける措置＞ ①住民については、既存住民基本台帳システムと連携される。
リスクへの対策は十分か	[　　] ＜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： 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	＜情報連携基盤システム・中間サーバーにおける措置＞ ①住民については、既存住民基本台帳システムと連携されるため、本人確認は行わない。
個人番号の真正性確認の措置の内容	＜情報連携基盤システム・中間サーバーにおける措置＞ ①住民については、既存住民基本台帳システムと連携される。
特定個人情報の正確性確保の措置の内容	＜情報連携基盤システム・中間サーバーにおける措置＞ ①住民については、既存住民基本台帳システムと連携されるため、正確な情報となる。 ②住民以外の者については、情報連携基盤システムを利用する各事務において住民基本台帳ネットワークシステムを利用するなどして正確な情報に更新する。
その他の措置の内容	
リスクへの対策は十分か	[　　] ＜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	＜情報連携基盤システム・中間サーバーにおける措置＞ ①アクセス制御や暗号化を実施することにより、漏えい・紛失を防止する。
リスクへの対策は十分か	[　　] ＜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	

情報連携基盤システム及び中間サーバーで保有する宛名ファイルを利用する場合にはこのとおり記載すること。
（評価対象事務の他の特定個人情報ファイル（〇〇ファイル）に宛名ファイルに該当する項目を含める場合には、「宛名ファイル」と「〇〇ファイル」の記載内容を統合すること）

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	＜情報連携基盤システムにおける措置＞ ①許可のない業務システムや端末はシステムに接続できないように制限している。 ②許可のない業務システムや利用者は個人番号にアクセスできないように制限している。	
事務で使用するその他のシステムにおける措置の内容	＜〇〇システムにおける措置＞ ①個人番号を直接保有せず、限られた処理で情報連携基盤システムで保有する個人番号を参照することで、個人番号の利用を制限している。	
その他の措置の内容		
リスクへの対策は十分か	[ ] ＜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： 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	[ ] ＜選択肢＞ 1）行っている　2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ ①端末利用時には、利用者個人に付与されるIDとパスワード及び生体認証による二要素認証を実施する。 ②システム連携時には、システムの認証を実施する。	評価対象事務での措置の内容も記載すること。
アクセス権限の発効・失効の管理	[ ] ＜選択肢＞ 1）行っている　2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ ①発行 利用する情報、権限の種類、利用期間、事務の名称と内容、根拠法令等、利用者の範囲又は利用システム等に基づき設定する。 ②失効 利用期間満了時に失効される。 また、利用者の範囲から外れた職員（異動、退職等）は失効される。	評価対象事務での措置の内容も記載すること。
アクセス権限の管理	[ ] ＜選択肢＞ 1）行っている　2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ ①定期的にアクセス権限を確認し、不要となったアクセス権限は変更または削除する。	評価対象事務での措置の内容も記載すること。
特定個人情報の使用の記録	[ ] ＜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	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムで保有する特定個人情報の情報照会・提供記録を保管する。 ②①の記録には宛名番号（住登外者宛名番号）、成否、日時、所属、事務、事務手続、職員、システムID、特定個人情報、特定個人情報の項目を含む。（所属、職員等システム連携のため特定できない場合には、利用する業務システム側で特定できる記録を残す。） ③情報連携基盤システムで保有する申請情報及び申請処理状況のアクセス記録を保管する。 ④③の記録には成否、日時、所属、職員、システムIDの項目を含む。（所属、職員等システム連携のため特定できない場合には、利用する業務システム側で特定できる記録を残す。）	評価対象事務での措置の内容も記載すること。 （記録の点検についても記述すること。）
リスクへの対策は十分か	[ ] ＜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	＜情報連携基盤システムにおける措置＞ ①システムの操作ログ、特定個人情報ファイルのアクセスログを記録する。 ②許可のない情報にはアクセスできないように制限する。	評価対象事務での措置の内容も記載すること。
リスクへの対策は十分か	[ ] ＜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	＜情報連携基盤システム・中間サーバーにおける措置＞ ①情報連携基盤システム・中間サーバーを利用する端末では、許可のない外部記録媒体の使用を禁止する。 ②必要最低限の利用者又は業務システムに対して必要最低限の出力しかできないアクセス権を設定をする。	評価対象事務での措置の内容も記載すること。
リスクへの対策は十分か	[ ] ＜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		

①は個人番号を直接保有しない場合の記載例
評価対象事務で使用するシステムにおけるの措置の内容を記載すること。

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 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			
情報保護管理体制の確認	＜情報連携基盤システムにおける措置＞ ①委託契約の締結にあたり、体制の確認を行うとともに秘密保持に関する誓約の提出を求める。		評価対象事務での措置の内容も記載すること。
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＞ 1）制限している　　2）制限していない	
具体的な制限方法	＜情報連携基盤システムにおける措置＞ ①作業実施体制の提出を求める。 ②作業実施にあたり必要となる最低限の従事者に対して個別にアクセス権限を付与する。		評価対象事務での措置の内容も記載すること。
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＞ 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	＜情報連携基盤システムにおける措置＞ ①システムの操作ログ、アクセスログを記録する。 ②システムの操作ログ、アクセスログを7年間保存する。		評価対象事務での措置の内容も記載すること。
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	＜情報連携基盤システムにおける措置＞ ①提供を禁止する。 ②契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
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	＜情報連携基盤システムにおける措置＞ ①庁舎外への持ち出しを禁止する。 ②契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
特定個人情報の消去ルール	[　　]	＜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			
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	＜情報連携基盤システムにおける措置＞ ①番号利用法及び関連法令を遵守し、適正な管理のために必要な措置を講じること。 ②第三者に開示あるいは漏洩してはならないこと。 ③目的外に使用してはならないこと。 ④漏えい、滅失又は改ざんの防止に必要な措置を講じること。 ⑤許可なく複写・複製しないこと。 ⑥漏えい、滅失又は改ざん等の事故が生じ、又は生ずるおそれがあることを知ったときは、直ちに委託者に報告し、委託者の指示に従うこと。 ⑦従事者の教育を実施すること。		評価対象事務での措置の内容も記載すること。
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	[　　]	＜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	＜情報連携基盤システムにおける措置＞ ①許可のない再委託を禁止する。 ②特定個人情報の取扱いに関して委託先に課せられている事項と同一の事項を遵守を義務付ける。 ③契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
その他の措置の内容			
リスクへの対策は十分か	[　　]	＜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	[ ] ＜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	
特定個人情報の提供・移転に関するルール	[ ] ＜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	
その他の措置の内容	
リスクへの対策は十分か	[ ] ＜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	
リスクへの対策は十分か	[ ] ＜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	
リスクへの対策は十分か	[ ] ＜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	

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＞ 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： 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＞ 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： 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＞ 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＞ 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＞ 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＞ 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＞ 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
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	[ ]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 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	[ ]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[ ]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 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	[ ]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[ ]	<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
具体的な対策の内容	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムは、ガバメントクラウド及び庁舎内の情報管理室に設置し、情報管理室への入退室を厳重に管理する。 ②特定個人情報は、ガバメントクラウド及び情報管理室内に設置された機器に保存する。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記録媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 ＜ガバメントクラウドにおける措置＞ 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。	
⑥技術的対策	[ ]	<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
具体的な対策の内容	＜情報連携基盤システムにおける措置＞ ①セキュリティ機器等を導入し、アクセス制限、侵入検知及び侵入防止を行う。 ②ウイルス対策ソフトウェアを導入する。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、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。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜ガバメントクラウドにおける措置＞ 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。 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ついて【第2.1版】」（令和6年7月デジタル庁。以下「利用について」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（利用についてに規定する「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。 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。 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。 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。 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。 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。 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。	

評価対象事務での措置の内容も記載すること。
（業務システムで個人番号を直接保有しない場合には不要）

評価対象事務での措置の内容も記載すること。
（業務システムで個人番号を直接保有しない場合には不要）

⑦バックアップ	[ ]	<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
⑧事故発生時手順の策定・周知	[ ]	<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
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> 1）発生あり　2）発生なし
その内容	本市の事業の受託業者が、事業の参加者に対してアンケート調査の依頼を電子メールにて一括送信する際、本来「BCC」欄を使用すべきところ、誤って「宛先」欄を使用し、電子メールアドレス（121名分）を他の参加者から閲覧できる状態で送信した。	
再発防止策の内容	受託業者に対し、個人情報の取扱いについて誤りのないよう指示徹底した。 電子メールを一括送信する際は複数の職員で確認するように指導を行った。	
⑩死者の個人番号	[ ]	<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	<情報連携基盤システムにおける措置> ①死者以外の個人番号と同様に管理する。	
その他の措置の内容		
リスクへの対策は十分か	[ ]	<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	<情報連携基盤システムにおける措置> ①住民については、既存住民基本台帳システムと連携されるため、正確な情報となる。 ②住民以外の者については、情報連携基盤システムを利用する各事務において住民基本台帳ネットワークシステムを利用するなどして正確な情報に更新する。	
リスクへの対策は十分か	[ ]	<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	[ ]	<選択肢> 1）定めている　2）定めていない
手順の内容	<情報連携基盤システムにおける措置> ①不要となった情報は定期的（月1回）に削除する。 <ガバメントクラウドにおける措置> 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	[ ]	<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		

個人情報に関する重大事故については、このとおり記載すること。
（令和4年9月発生）

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。
（住基ネットを利用できない事務では②は記載しないこと。）

評価対象事務での措置の内容も記載すること。
（業務システムで個人番号を直接保有しない場合には不要）

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	
2．〇〇ファイル	
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	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ マニュアルやweb上で、個人番号の提出が必要な者の要件を明示、周知し、本人以外の情報の入手を防止する。
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	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ 住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。
その他の措置の内容	
リスクへの対策は十分か	[　　] ＜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：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。 ②サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。
リスクへの対策は十分か	[　　] ＜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：　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	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ 住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証（有効性確認、改ざん検知等）を実施することとなる。これにより、本人確認を実施する。
個人番号の真正性確認の措置の内容	
特定個人情報の正確性確保の措置の内容	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ 個人番号カード内の記憶領域に格納された個人番号を申請フォームに自動転記を行うことにより、不正確な個人番号の入力を抑止する措置を講じている。
その他の措置の内容	
リスクへの対策は十分か	[　　] ＜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	＜情報連携基盤システムにおける措置＞ サービス検索・電子申請機能と申請管理システムの間にDMZを設けることにより、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また、FWで外部接続先との通信を制限している。 ＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。
リスクへの対策は十分か	[　　] ＜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	

情報連携基盤システム（情報照会・提供）、中間サーバー（情報提供）、情報提供ネットワークシステム（情報照会）を利用する場合には情報連携基盤システム及び中間サーバーに関する委託についてこのとおり記載すること。
ぴったりサービス（サービス検索・電子申請機能）を利用する場合には、このような観点から記載するすること。

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	＜情報連携基盤システムにおける措置＞ ①許可のない業務システムや端末はシステムに接続できないように制限している。 ②許可のない業務システムや利用者は個人番号にアクセスできないように制限している。	
事務で使用するその他のシステムにおける措置の内容	＜○○システムにおける措置＞ ①個人番号を直接保有せず、限られた処理で情報連携基盤システムで保有する個人番号を参照することで、個人番号の利用を制限している。	
その他の措置の内容		
リスクへの対策は十分か	[ ] ＜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： 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	[ ] ＜選択肢＞ 1）行っている 2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ ①端末利用時には、利用者個人に付与されるIDと、パスワード及び生体認証による二要素認証を実施する。 ②システム連携時には、システムの認証を実施する。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①サービス検索・電子申請機能をLGWAN接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 ②なりすましによる不正を防止する観点から共用IDの利用を禁止する。	
アクセス権限の発効・失効の管理	[ ] ＜選択肢＞ 1）行っている 2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ ①発行 利用する情報、権限の種類、利用期間、事務の名称と内容、根拠法令等、利用者の範囲又は利用システム等に基づき設定する。 ②失効 利用期間満了時に失効される。 また、利用者の範囲から外れた職員（異動、退職等）は失効される。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①発効 アクセス権限が必要となった場合、ユーザID管理者が事務に必要となる情報にアクセスできるユーザIDを発効する。 ユーザID管理者が各事務に必要となるアクセス権限の管理表を作成する。 アクセス権限の付与を必要最低限とする。 ②失効 定期的又は異動/退職等のイベントが発生したタイミングで、権限を有していた職員の異動/退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。	
アクセス権限の管理	[ ] ＜選択肢＞ 1）行っている 2）行っていない	
具体的な管理方法	＜情報連携基盤システムにおける措置＞ 定期的にアクセス権限を確認し、不要となったアクセス権限は変更または削除する。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ 定期的にユーザID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザID管理者が確認を行う。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。	

①は個人番号を直接保有しない場合の記載例
評価対象事務で使用するシステムにおけるの措置の内容を記載すること。

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。

特定個人情報の使用の記録	[　　]	＜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	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムで保有する特定個人情報の情報照会・提供記録を保管する。 ②①の記録には宛名番号、住登外者宛名番号、成否、日時、所属、事務、事務手続、職員、システムID、特定個人情報、特定個人情報の項目を含む。（所属、職員等システム連携のため特定できない場合には、利用する業務システム側で特定できる記録を残す。）	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ②アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ③定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。	
その他の措置の内容		
リスクへの対策は十分か	[　　]	＜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	＜情報連携基盤システムにおける措置＞ ①システムの操作ログ、アクセスログを記録する。 ②許可のない情報にはアクセスできないように制限している。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①サービス検索・電子申請機能へアクセスできる端末を制限する。 ②外部記録媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に○○○の責任者の承認を得たうえで複製する。なお、外部記録媒体は限定されたUSBメモリ等のみを使用する。 ③外部記録媒体内のデータは暗号化する。	
リスクへの対策は十分か	[　　]	＜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	＜情報連携基盤システム・中間サーバーにおける措置＞ ①情報連携基盤システム・中間サーバーを利用する端末では、許可のない外部記録媒体の使用を禁止する。 ②必要最低限の利用者又は業務システムに対して必要最低限の出力しかできないアクセス権を設定をする。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。 ②アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、LGWAN接続端末への保存や外部記録媒体への書き出し等ができるようシステム的に制御する。 ③外部記録媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に○○○の責任者の承認を得たうえで複製する。なお、外部記録媒体は限定されたUSBメモリ等のみを使用する。 ④外部記録媒体内のデータは暗号化する。	
リスクへの対策は十分か	[　　]	＜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		

評価対象事務での措置の内容も記載すること。
（記録の点検についても記述すること。）

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。

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 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			
情報保護管理体制の確認	＜情報連携基盤システムにおける措置＞ ①委託契約の締結にあたり、体制の確認を行うとともに秘密保持に関する誓約の提出を求める。		評価対象事務での措置の内容も記載すること。
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＞ 1）制限している　2）制限していない	
具体的な制限方法	＜情報連携基盤システムにおける措置＞ ①作業実施体制の提出を求める。 ②作業実施にあたり必要となる最低限の従事者に対して個別にアクセス権限を付与する。		評価対象事務での措置の内容も記載すること。
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＞ 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	＜情報連携基盤システムにおける措置＞ ①システムの操作ログ、アクセスログを記録している。 ②システムの操作ログ、アクセスログを7年間保存する。		評価対象事務での措置の内容も記載すること。
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	＜情報連携基盤システムにおける措置＞ ①提供を禁止する。 ②契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
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	＜情報連携基盤システムにおける措置＞ ①庁舎外への持ち出しを禁止する。 ②契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
特定個人情報の消去ルール	[　]	＜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			
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	＜情報連携基盤システムにおける措置＞ ①番号利用法及び関連法令を遵守し、適正な管理のために必要な措置を講じること。 ②第三者に開示あるいは漏洩してはならないこと。 ③目的外に使用してはならないこと。 ④漏えい、滅失又は改ざんの防止に必要な措置を講じること。 ⑤許可なく複写・複製しないこと。 ⑥漏えい、滅失又は改ざん等の事故が生じ、又は生ずるおそれがあることを知ったときは、直ちに委託者に報告し、委託者の指示に従うこと。 ⑦従事者の教育を実施すること。		評価対象事務での措置の内容も記載すること。
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	[　]	＜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	＜情報連携基盤システムにおける措置＞ ①許可のない再委託を禁止する。 ②特定個人情報の取扱いに関して委託先に課せられている事項と同一の事項を遵守を義務付ける。 ③契約に基づき遵守状況の報告を求めるとともに、実地確認調査を実施する。		評価対象事務での措置の内容も記載すること。
その他の措置の内容			
リスクへの対策は十分か	[　]	＜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	[　]	＜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	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムを利用した特定個人情報の提供・移転は、全て情報照会・提供記録を取得する。 ②取得した情報照会・提供記録は7年間保存する。	
特定個人情報の提供・移転に関するルール	[　]	＜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	＜〇〇システムにおける措置＞ ①情報連携基盤システムを利用することで、外部記録媒体を利用した特定個人情報の移転・提供は行わない。 ② ＜情報連携基盤システムにおける措置＞ ①移転・提供元によって許可された移転・提供先にのみ移転・提供する。 ②定期的に移転・提供元及び移転・提供先に確認する。	
その他の措置の内容		
リスクへの対策は十分か	[　]	＜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	＜〇〇システムにおける措置＞ ①情報連携基盤システムを通じて特定個人情報の提供・移転を行うことにより、不適切な方法で提供・移転が行われることを防止する。 ＜情報連携基盤システムにおける措置＞ ①許可のない業務システムや端末はシステムに接続できないように制限している。 ②許可のない特定個人情報にはアクセスできないように制限している。	
リスクへの対策は十分か	[　]	＜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	＜〇〇システムにおける措置＞ ①情報連携基盤システムを通じて特定個人情報の提供・移転を行うことにより、誤った情報の提供・移転や誤った相手への提供・移転を防止する。 ＜情報連携基盤システムにおける措置＞ ①許可のない業務システムや端末はシステムに接続できないように制限している。 ②許可のない特定個人情報にはアクセスできないように制限している。	
リスクへの対策は十分か	[　]	＜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		

移転・提供しない場合は記載不要（〇印を選択すると、グレーアウトされる）

情報連携基盤システムを経由しない特定個人情報の提供・移転がある場合には、関係する業務システム等における措置の内容を記載すること。

評価対象事務での措置の内容も記載すること。
＜〇〇システムにおける措置＞の内容は、情報連携基盤システムによる情報連携に完全対応した場合の記載例

評価対象事務での措置の内容も記載すること。
＜〇〇システムにおける措置＞の内容は、情報連携基盤システムによる情報連携に完全対応した場合の記載例

評価対象事務での措置の内容も記載すること。
＜〇〇システムにおける措置＞の内容は、情報連携基盤システムによる情報連携に完全対応した場合の記載例

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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号利用法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号利用法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報 照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
リスクへの対策は十分か	[　] ＜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： 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	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　] ＜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： 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	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[　] ＜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

接続しない場合には記載不要（記載不要箇所はグレーアウトされる）

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	＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
リスクへの対策は十分か	[ ] ＜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	＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③例えばDVや虐待等の被害者（DVや虐待等の被害を受ける恐れがある者を含む）の情報など人の生命、健康、生活または財産を害する恐れがある情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 ＜中間サーバーの運用における措置＞ ①必要に応じて中間サーバー側で取得した情報提供記録を確認する。
リスクへの対策は十分か	[ ] ＜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	＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（※）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
リスクへの対策は十分か	[　　] ＜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	＜情報連携基盤システムにおける措置＞ ①中間サーバーに保存する特定個人情報を適切な頻度で更新する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[　　] ＜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
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	
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	

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	[ ]	＜選択肢＞ 1）特に力を入れて遵守している　2）十分に遵守している 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	[ ]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 3）十分に整備していない
③安全管理規程	[ ]	＜選択肢＞ 1）特に力を入れて整備している　2）十分に整備している 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	[ ]	＜選択肢＞ 1）特に力を入れて周知している　2）十分に周知している 3）十分に周知していない
⑤物理的対策	[ ]	＜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
具体的な対策の内容	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムは、ガバメントクラウド及び庁舎内の情報管理室に設置しており、情報管理室への入退室を厳重に管理する。 ②特定個人情報は、ガバメントクラウド及び情報管理室内に設置された機器に保存される。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記録媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 ＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ②外部記録媒体については、限定されたUSBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 ＜ガバメントクラウドにおける措置＞ 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。 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。	

評価対象事務での措置の内容も記載すること。

⑥技術的対策		[　　] ＜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
	具体的な対策の内容	＜情報連携基盤システムにおける措置＞ ①セキュリティ機器等を導入し、アクセス制限、侵入検知及び侵入防止を行う。 ②ウイルス対策ソフトウェアを導入する。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、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。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①LGWAN接続端末へのウィルス検出ソフトウェア等の導入により、ウィルス定義ファイルの定期的な更新及びウィルスチェックを行い、マルウェア検出を行う。 ②サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ＜ガバメントクラウドにおける措置＞ 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。 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ついて【第2.1版】（令和6年7月デジタル庁。以下「利用について」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（利用について）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。 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。 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。 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。 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。 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。 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。
⑦バックアップ		[　　] ＜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
⑧事故発生時手順の策定・周知		[　　] ＜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
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＞ 1）発生あり　2）発生なし
	その内容	本市の事業の受託業者が、事業の参加者に対してアンケート調査の依頼を電子メールにて一括送信する際、本来「BCC」欄を使用すべきところ、誤って「宛先」欄を使用し、電子メールアドレス（121名分）を他の参加者から閲覧できる状態で送信した。
	再発防止策の内容	受託業者に対し、個人情報の取扱いについて誤りのないよう指示徹底した。 電子メールを一括送信する際は複数の職員で確認するように指導を行った。
⑩死者の個人番号		[　　] ＜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	
その他の措置の内容		
リスクへの対策は十分か		[　　] ＜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

個人情報に関する重大事故については、このとおり記載すること。
（令和4年9月発生）

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	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ・LGWAN接続端末は、基本的には、個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。	
リスクへの対策は十分か	[ ]	＜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	[ ]	＜選択肢＞ 1）定めている　2）定めていない
手順の内容	＜情報連携基盤システムにおける措置＞ ①保管期間が過ぎた情報は定期的（月1回）に削除する。 ②接続する業務システムからの不要となった情報の削除要求に基づき、削除する。	
	＜ぴったりサービス（サービス検索・電子申請機能）における措置＞ ①LGWAN接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。 ②外部記録媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。	
	＜ガバメントクラウドにおける措置＞ 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	[ ]	＜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		

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	[　　]	＜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
具体的なチェック方法	＜情報連携基盤システムにおける措置＞ ①情報連携基盤システムの運用及び情報連携基盤システムでの特定個人情報ファイルの取り扱いが、本評価書及び運用規則等のとおり適切に実施されていることを確認するために、情報連携基盤システムの運用に携わる職員については年一回、システム開発・運用保守業者については月一回の自己点検を実施することとしている。 ＜中間サーバー・プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。	
②監査	[　　]	＜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
具体的な内容	＜情報連携基盤システムにおける措置＞ ①「名古屋市における特定個人情報の適正な取扱いに関する方針」に基づき、情報連携基盤システムにおける特定個人情報の管理の状況の点検又は情報セキュリティ監査を実施する。 ②①の実施結果に応じて必要な改善措置を講じる。 ＜中間サーバー・プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ＜ガバメントクラウドにおける措置＞ 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	[　　]	＜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
具体的な方法	＜名古屋市における措置＞ ①「名古屋市における特定個人情報の適正な取扱いに関する方針」に基づき、特定個人情報の保護責任者、特定個人情報を取扱うシステム所管課長及び所管課長、各事務取扱担当者等に対して、特定個人情報の適正な管理に関する研修をおおむね1年ごとに行う。 ②「名古屋市における特定個人情報の適正な取扱いに関する方針」に基づき、特定個人情報を取扱うシステムを利用する職員に対して、システムの運用及びセキュリティ対策に関する研修をおおむね1年ごとに行う。 ③「名古屋市における特定個人情報の適正な取扱いに関する方針」に基づき、その他の特定個人情報を取扱う職員に対して特定個人情報の安全管理に関する研修をおおむね1年ごとに実施する。 ＜情報連携基盤システムにおける措置＞ ①委託業者に対して、番号利用法及び関連法令の順守、機密保持及び従事者への情報の取扱いに関する教育を求める。 ＜中間サーバー・プラットフォームにおける措置＞ ①IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資 材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。 ＜違反行為を行った場合の措置＞ 違反行為を行った場合は、関係法令等に基づき厳正に対処する。	

評価対象事務での措置の内容も記載すること。
点検の頻度については、例えば「月一回」などできるだけ具体的に記載したうえで、誰が何について点検を実施するかについてもできる限り記載すること。

評価対象事務での措置の内容も記載すること。

評価対象事務での措置の内容も記載すること。

3. その他のリスク対策

＜中間サーバー・プラットフォームにおける措置＞
①中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシーの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。

＜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。

評価対象事務での措置の内容も記載すること。

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	郵便番号460-8508 名古屋市中区三の丸三丁目1番1号 名古屋市スポーツ市民局市民生活部市政情報課
②請求方法	個人情報の保護に関する法律に基づき、必要事項を記載した開示・訂正・利用停止請求書を提出する。
特記事項	開示請求について、市公式ウェブサイト上に、請求先、請求方法、請求書様式等を掲載している。
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　　行っている　　]　＜選択肢＞ 1) 行っている　2) 行っていない
個人情報ファイル名	○○ファイル
公表場所	市民情報センター、市公式ウェブサイト
⑤法令による特別の手続	-
⑥個人情報ファイル簿への不記載等	-

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	
②対応方法	

Ⅵ　評価実施手続

1．基礎項目評価	
①実施日	
②しきい値判断結果	[　　] ＜選択肢＞ 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 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） 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） 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	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3．第三者点検	
①実施日	
②方法	
③結果	
4．特定個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②特定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