

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
10	町田市 予防接種事務 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

町田市は予防接種事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

町田市情報セキュリティポリシー

1 目的

町田市情報セキュリティポリシーは、様々な脅威に対する抑止、防止、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針であり、情報セキュリティを実践するに当たっての基本的な考え方及び方策を定めることによって、市が保有する情報資産の機密性、完全性及び可用性を維持し、市民からの継続的な信頼を獲得することを目的とする。

評価実施機関名

町田市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和7年4月1日

項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
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
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 変更箇所

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	予防接種事務						
②事務の内容 ※	<p>町田市は、感染のおそれがある疾病の発生及びまん延を予防するために、公衆衛生の見地から、対象者に対して、期日又は期間を指定して予防接種(定期の予防接種及び新型インフルエンザ等の予防接種、新型コロナウイルス感染症予防接種を指す。)の実施その他の必要な措置を講ずることにより、市民の健康の保持に寄与するとともに、予防接種による健康被害の迅速な救済を図るため、「予防接種法」及び「新型インフルエンザ等特別措置法」、「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(以下「番号法」という。)の規定に従い、特定個人情報を利用する事務において、特定個人情報ファイルを以下の事務で取り扱う。</p> <ol style="list-style-type: none"> 各種予防接種の案内 予防接種の接種対象者への接種勧奨を行う 予防接種履歴の管理 予防接種の実施後に接種記録等を登録、管理し、他市区町村へ接種記録の照会・提供を行う。新型コロナウイルス感染症対策に係る予防接種事務においては、ワクチン接種記録システム(VRS)へ予防接種対象者及び発行した接種券の登録を行う。また、予防接種の実施後に、接種者からの申請に基づき、新型コロナウイルス感染症予防接種証明書の交付を行う。 実費徴収に関する事務 予防接種にかかる自己負担金の免除を希望する者に対し、実費徴収の有無を決定する(B類疾病に関する予防接種に限る。))。 給付の支給(予防接種法に基づく予防接種の場合) <ol style="list-style-type: none"> 健康被害が生じた場合、住民(被害者)から健康被害の給付申請を受理 申請内容を本市で審議した後、申請書類等を国へ進達 健康被害が認定された場合は、被害者に対して給付金を支給 給付の支給(予防接種法に基づかない予防接種の場合) <ol style="list-style-type: none"> 健康被害が生じた場合、町田市予防接種事故災害補償規則に基づき、住民(被害者)に対して、補償金等を支給 接種券の作成 年齢・性別・個人接種歴から、必要な予防接種の接種券を作成 予防接種証明書の作成 個人接種歴を使用して、予防接種証明書を出力 各種統計の作成 各種統計を作成 						
③対象人数	<p>[30万人以上]</p> <p style="text-align: right;">＜選択肢＞</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;">1) 1,000人未満</td> <td style="width: 50%;">2) 1,000人以上1万人未満</td> </tr> <tr> <td>3) 1万人以上10万人未満</td> <td>4) 10万人以上30万人未満</td> </tr> <tr> <td>5) 30万人以上</td> <td></td> </tr> </table>	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	
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							

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	健康管理システム
②システムの機能	<p>本システムの予防接種事務に関する主な機能は次のとおり。</p> <ol style="list-style-type: none"> 対象者管理機能 接種勧奨を行うための個人情報を管理する機能。 接種履歴管理機能 予防接種履歴を登録、管理する機能。 統合連携基盤との連携機能
③他のシステムとの接続	<p>[] 情報提供ネットワークシステム [] 庁内連携システム</p> <p>[] 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</p> <p>[] 宛名システム等 [] 税務システム</p> <p>[○] その他 (統合連携基盤、ワクチン接種記録システム(VRS))</p>
システム2～5	

システム2	
①システムの名称	ワクチン接種記録システム(VRS)
②システムの機能	<p>本システムの予防接種事務に関する主な機能は次のとおり。</p> <ol style="list-style-type: none"> 1. 接種対象者・接種券発行管理 2. 接種記録の管理 3. 転出/死亡時等のフラグ設定 4. 他市区町村への接種記録の照会・提供 5. 新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会 6. 新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 7. 新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施
③他のシステムとの接続	<p>[] 情報提供ネットワークシステム [] 庁内連携システム</p> <p>[] 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</p> <p>[] 宛名システム等 [] 税務システム</p> <p>[○] その他 (健康管理システム)</p>
システム3	
①システムの名称	統合連携基盤
②システムの機能	<p>本システムの主な機能は次のとおり。</p> <ol style="list-style-type: none"> 1. 団体内統合宛名番号付番機能 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し、各業務システムの宛名番号と紐づけて管理する。 2. 中間サーバー情報連携機能 各業務システムと中間サーバーとの情報連携を行う。 3. 統合DB機能 一般財団法人全国地域情報化推進協会(APPLIC)が定める「地域情報プラットフォーム標準仕様」に準拠した業務情報を管理し、連携する。 (統合連携基盤は「③他のシステムとの接続」における「庁内連携システム」と「宛名システム等」の機能を兼ねている。)
③他のシステムとの接続	<p>[] 情報提供ネットワークシステム [] 庁内連携システム</p> <p>[] 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</p> <p>[] 宛名システム等 [] 税務システム</p> <p>[○] その他 (中間サーバー、健康管理システム、国保システム、後期システム、生保システム等)</p>

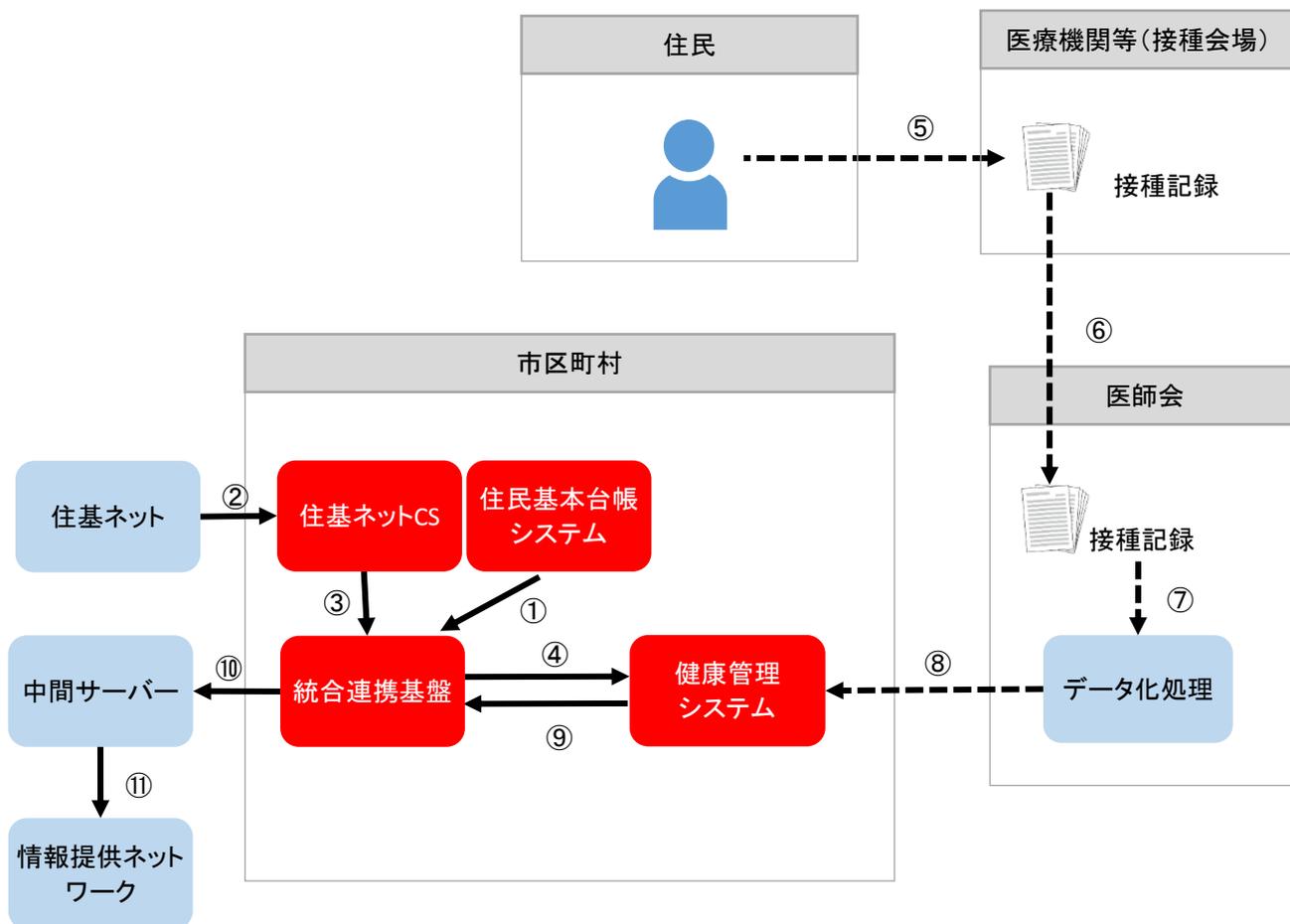
システム4									
①システムの名称	中間サーバー								
②システムの機能	<p>本システムの主な機能は次のとおり。</p> <ol style="list-style-type: none"> 1. 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 2. 情報照会機能 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 3. 情報提供機能 情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 4. 既存システム接続機能 中間サーバーと既存システム、宛名システム及び住民記録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 特定個人情報を副本として保存・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照合リストを管理する機能。 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 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う機能。 								
③他のシステムとの接続	<table border="0"> <tr> <td><input type="checkbox"/> 情報提供ネットワークシステム</td> <td><input type="checkbox"/> 庁内連携システム</td> </tr> <tr> <td><input type="checkbox"/> 住民基本台帳ネットワークシステム</td> <td><input type="checkbox"/> 既存住民基本台帳システム</td> </tr> <tr> <td><input type="checkbox"/> 宛名システム等</td> <td><input type="checkbox"/> 税務システム</td> </tr> <tr> <td colspan="2"><input type="checkbox"/> その他 (統合連携基盤)</td> </tr> </table>	<input type="checkbox"/> 情報提供ネットワークシステム	<input type="checkbox"/> 庁内連携システム	<input type="checkbox"/> 住民基本台帳ネットワークシステム	<input type="checkbox"/> 既存住民基本台帳システム	<input type="checkbox"/> 宛名システム等	<input type="checkbox"/> 税務システム	<input type="checkbox"/> その他 (統合連携基盤)	
<input type="checkbox"/> 情報提供ネットワークシステム	<input type="checkbox"/> 庁内連携システム								
<input type="checkbox"/> 住民基本台帳ネットワークシステム	<input type="checkbox"/> 既存住民基本台帳システム								
<input type="checkbox"/> 宛名システム等	<input type="checkbox"/> 税務システム								
<input type="checkbox"/> その他 (統合連携基盤)									
システム6～10									
システム11～15									
システム16～20									
3. 特定個人情報ファイル名									
予防接種ファイル									
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	<ul style="list-style-type: none"> ・予防接種の対象者、予防接種の実施記録等の情報の正確な把握かつ適正な管理を行う。 ・個人の特定を正確かつ効率的に行う。 ・番号法第19条第8号及び第9号に基づき、情報提供ネットワークシステムを通じた情報照会、情報提供業務を行う。 								
②実現が期待されるメリット	<ul style="list-style-type: none"> ・予防接種の対象者であることを確認し、対象者と受けた接種記録を紐づけることで、接種記録の管理、保管等について効率的な事務が可能となる。 ・対象者の接種歴を管理することで、未接種者を迅速に把握でき、感染症の発生及びまん延防止のために確保すべき一定の予防接種率となるよう接種率向上の取り組みを強化できる。 ・個人を特定する際の正確性が向上すること、また、事務の効率化に資することが期待できる。 ・住民票の写し等に代えて本人確認情報を利用することにより、これまでに窓口で提出が求められていた行政機関が発行する添付書類(住民票の写し等)の省略が図られ、もって住民の負担軽減(各機関を訪問し、証明書等を入手する金銭的、時間的コストの節約)につながるが見込まれる。 ・個人番号を保有するファイルを局所化し、漏洩リスクを低減できる。 								

5. 個人番号の利用 ※	
法令上の根拠	<p>番号法</p> <ul style="list-style-type: none"> ・第9条第1項(利用範囲)別表14の項(予防接種法) ・第9条第1項(利用範囲)別表126の項(予防接種法) ・第19条第6号(委託先への提供) ・第19条第8号(特定個人情報の提供の制限) ・第19条第16号(新型コロナウイルス感染症対策に係る予防接種事務におけるワクチン接種記録システム(VRS)を用いた情報提供・照会のみ) <p>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</p> <ul style="list-style-type: none"> ・第10条(予防接種法) ・第67条の2(新型インフルエンザ等対策特別措置法)
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	<p>[実施する]</p> <p style="text-align: right;"><選択肢> 1) 実施する 2) 実施しない 3) 未定</p>
②法令上の根拠	<p>番号法</p> <ul style="list-style-type: none"> ・第19条第8号に基づく主務省令第2条の表25、27、28、29の項(予防接種法) ・第19条第8号に基づく主務省令第2条の表25(新型インフルエンザ等対策特別措置法) <p>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二の主務省令で定める事務及び情報を定める命令</p> <ul style="list-style-type: none"> ・第12条の2、第12条の3、第13条、第13条の2(予防接種法) ・第59条の2(新型インフルエンザ等対策特別措置法)
7. 評価実施機関における担当部署	
①部署	保健所保健予防課
②所属長の役職名	保健所保健予防課長
8. 他の評価実施機関	

(別添1) 事務の内容

添付資料のとおり

(備考)



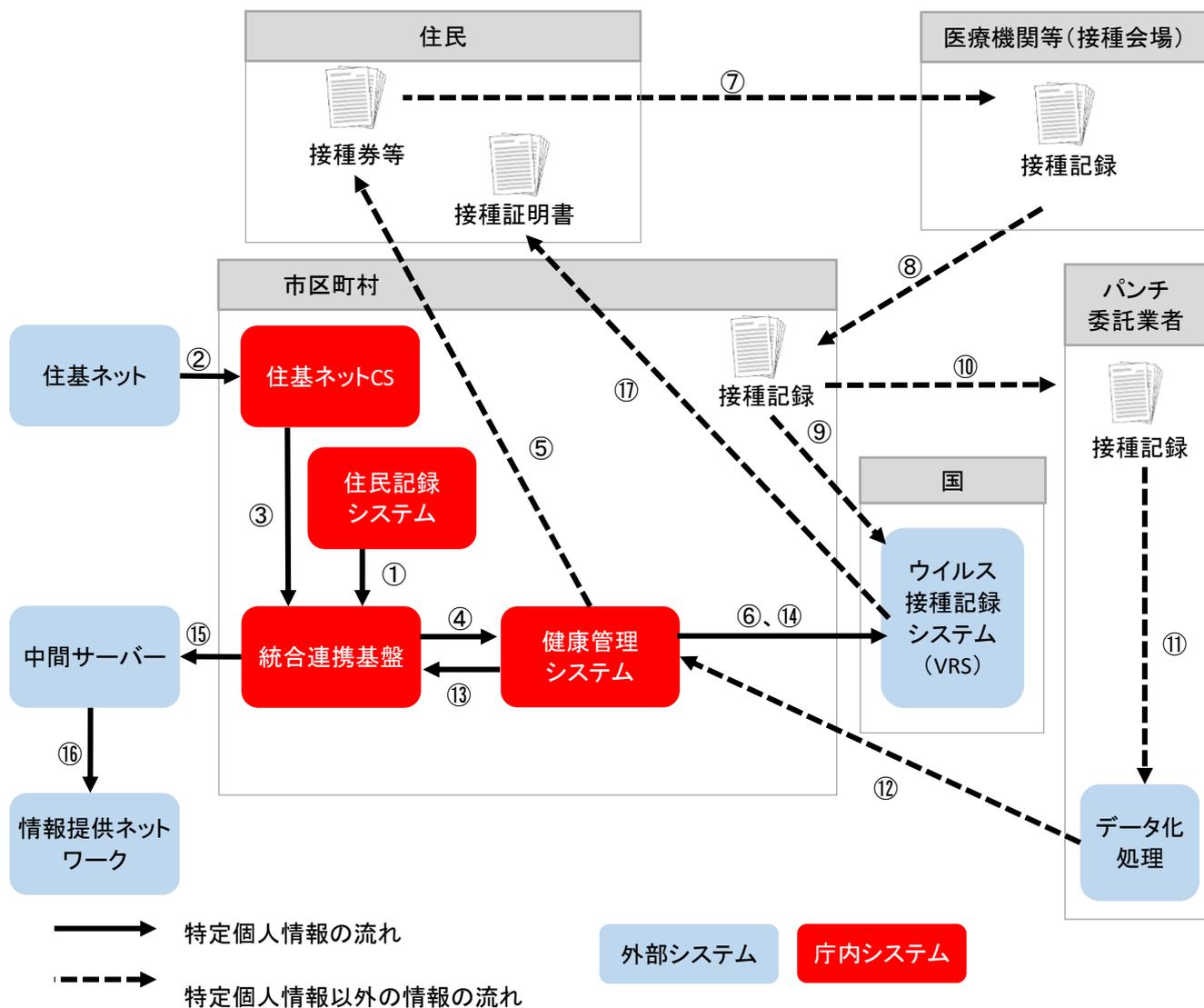
————→ 特定個人情報の流れ

- - - - - 特定個人情報以外の情報の流れ

外部システム

庁内システム

- ①住民情報が統合連携基盤に連携される。
- ②③住登外者情報が統合連携基盤に連携される。
- ④予防接種対象者の特定個人情報が統合連携基盤から取得される。
- ⑤予防接種のための受診。接種費用の自己負担免除を希望する場合、必要書類が提出される。
- ⑥接種記録が医師会に送付される。
- ⑦接種記録がデータ化される。
- ⑧データ化された接種記録が健康管理システムに取り込まれる。
- ⑨接種記録が統合連携基盤に連携される。
- ⑩⑪他市区町村からの照会に応じて接種記録が提供される。



- ①住民情報が統合連携基盤に連携される。
- ②③住登外者情報が統合連携基盤に連携される。
- ④予防接種対象者の特定個人情報が統合連携基盤から取得される。
- ⑤予防接種対象者に接種券等が送付される。
- ⑥予防接種対象者情報がウイルス接種記録システム (VRS) に登録される。
- ⑦予防接種のために受診し、接種券等が提出される。
- ⑧接種記録が送付される。
- ⑨接種記録がVRSに登録される。
- ⑩接種記録がパンチ委託業者に送付される。
- ⑪接種記録がデータ化される。
- ⑫データ化された接種記録が健康管理システムに取り込まれる。
- ⑬接種記録が統合連携基盤に連携される。
- ⑭接種記録がVRSに登録される。
- ⑮⑯他市区町村からの照会に応じて接種記録が提供される。
- ⑰ワクチン接種証明書が交付される。

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	
予防接種ファイル	
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	[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
③対象となる本人の範囲 ※	予防接種事業の対象者
その必要性	予防接種事業の対象者であることの確認、対象者の接種記録を適正に管理・保管するために必要。
④記録される項目	[10項目以上50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 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 4情報(氏名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 (世帯構成情報、外国人情報)
その妥当性	<ul style="list-style-type: none"> ・識別情報: 予防接種事業の対象者を特定するために必要 ・連絡先等情報: 予防接種事業の対象者であることを確認し、接種履歴を入力・管理するために必要 ・業務関係情報: 予防接種履歴の管理、及び勧奨を適正に行うために必要
全ての記録項目	別添2を参照。
⑤保有開始日	平成28年3月19日
⑥事務担当部署	保健所保健予防課

3. 特定個人情報の入手・使用	
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 (団体内の対応部署) <input type="checkbox"/> 行政機関・独立行政法人等 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 (市町村) <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 (医療機関)
②入手方法	<input type="checkbox"/> 紙 [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ <input type="checkbox"/> 電子メール [<input type="checkbox"/>] 専用線 [<input type="checkbox"/>] 庁内連携システム <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 (ワクテン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム)
③入手の時期・頻度	<ul style="list-style-type: none"> ・住民登録者は住民基本台帳システムから1日1回、システム間の連携により自動的に入手する。 ・住民登録外者は本人または本人の代理人から紙書類により入手する。 ・予診票の接種記録については、町田市医師会から月単位で入手する。 ・新型コロナウイルス感染症対策に係る予防接種事務においては、本市への転入者について転出元市区町村への接種記録の照会が必要になる都度、他市区町村から接種記録の照会を受ける都度、および新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合であって接種記録の照会が必要になる都度。
④入手に係る妥当性	<ul style="list-style-type: none"> ・個人を特定し、適正に予防接種情報を管理する必要がある。 ・新型コロナウイルス感染症対策に係る予防接種事務においては、本市への転入者について、転出元市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。(番号法第19条第16号) ・新型コロナウイルス感染症対策に係る予防接種事務においては、本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために、他市区町村から個人番号を入手する。(番号法第19条第16号) ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。

⑤本人への明示		<ul style="list-style-type: none"> ・本人または本人の代理人から特定個人情報の提供を受ける場合は、当該事務が番号法第9条別表1の10項で定める個人番号利用事務であること及び個人番号の利用目的を説明する。 ・個人番号及び四情報は住民基本台帳法で定義する本人確認情報であり、整備法第19条の定めにより改正される住民基本台帳法の別表第3の5の5の項、及び別表第5の6の3の項において、当該事務で本人確認情報を使用して良い旨が明示されている。 ・書面提出などによる入手のため本人または本人の代理人に直接説明できない場合にあっては、本人確認情報の使用については上記のとおり明示されている。 ・当市への転入者について、接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。 ・電子交付アプリにより、予防接種証明書の電子申請を受ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受ける場合においては、利用規約を表示し、同意を得てから入手する。
⑥使用目的 ※		対象者の資格管理、接種記録の管理・保管に係る事務を適正かつ公正に行うため
変更の妥当性		
⑦使用の主体	使用部署 ※	保健所保健予防課
	使用者数	<div style="display: flex; align-items: center;"> <div style="margin-right: 20px;">[10人以上50人未満]</div> <div style="border: 1px solid black; padding: 5px;"> <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 </div> </div>
⑧使用方法 ※		<ul style="list-style-type: none"> ・健康管理システムに接種記録を登録し、接種記録の管理及び保管を行う。 ・新型コロナウイルス感染症対策に係る予防接種事務においては、当市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ・新型コロナウイルス感染症対策に係る予防接種事務においては、当市からの転出者について、転出先市区町村へ当市での接種記録を提供するために特定個人情報を使用する。 ・新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。 ・申請書で公金受取口座での受取希望(同意)があった場合、情報提供ネットワークシステムから公金受取口座情報を取得し、申請書の口座情報欄に転記する。
情報の突合 ※		<ul style="list-style-type: none"> ・予診票に記入された住所、氏名、生年月日等と突合し、接種対象者かどうか確認し突合する。 ・新型コロナウイルス感染症対策に係る予防接種事務においては、当市区町村からの転出者について、当市区町村での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、当市区町村の接種記録と突合する。
情報の統計分析 ※		個人を特定する統計は行わない。
権利利益に影響を与え得る決定 ※		権利利益に影響を与える決定は行わない。
⑨使用開始日		平成28年3月22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> 1) 委託する 2) 委託しない (4) 件	
委託事項1	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	
①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	
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 ※	予防接種法等関連法令に定められた予防接種の対象者	
その妥当性	ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	
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 LG-WANを用いた提供(VRS本体、コンビニ交付関連機能)、本人からの電子交付アプリを用いた提供(新型コロナウイルス感染症予防接種証明書電子交付機能)	
⑤委託先名の確認方法	下記、「⑥委託者名」の項の記載より確認できる。	
⑥委託先名	株式会社ミラボ	
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2～5	
委託事項2	健康管理システムの保守業務
①委託内容	当該システムを安定的に使用するため、障害対応や法改正対応等によるシステムの構成変更対応等を実施する。
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 [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 ※ 特定個人情報ファイルの範囲と同様
	その妥当性 システムの安定した稼働のため、システムに専門的な知識を有する民間事業者に委託している。ただし、通常業務では特定個人情報ファイルを取り扱わない。
③委託先における取扱者数	[10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 原則、特定個人情報ファイルの提供は行わず、障害等の緊急時及びシステム [○] その他 (ムの運用・保守を行ううえで必要不可欠な場合で、担当課が許可した場合) にのみ、管理端末にてシステムの直接操作を認めている。
⑤委託先名の確認方法	町田市情報公開条例に基づき情報提供している。
⑥委託先名	株式会社両備システムズ
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 原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項 上記、再委託承認書の内容による。

委託事項3		健康管理システムの運用業務
①委託内容		当該システムを効率的に使用するため、一括処理の実行と帳票印刷及び死活監視を実施する。
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	<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 ※	特定個人情報ファイルの範囲と同様
	その妥当性	システムの安定した稼働のため、システムに専門的な知識を有する民間事業者に委託している。ただし、通常業務では特定個人情報ファイルを取り扱わない。
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 (原則、特定個人情報ファイルの提供は行わず、障害等の緊急時及びシステムの運用・保守を行ううえで必要不可欠な場合で、担当課が許可した場合) にのみ、管理端末にてシステムの直接操作を認めている。
⑤委託先名の確認方法		町田市情報公開条例に基づき情報提供している。
⑥委託先名		株式会社 エヌ・ティ・ティ・データ
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	原則、業務の全部または一部を第三者に再委託してはならない。ただし、必要不可欠な場合は、情報セキュリティ確保・個人情報保護のための特記仕様書に基づき、委託先が再委託承認申請書にて申請し、市が再委託を認めた上で、再委託承認書を送付する。
	⑨再委託事項	上記、再委託承認書の内容による。

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	[<input checked="" type="checkbox"/>] 提供を行っている (74) 件 [] 移転を行っている () 件 [] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号
②提供先における用途	予防接種の実施に関する事務
③提供する情報	予防接種情報
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] <small><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</small>
⑤提供する情報の対象となる本人の範囲	予防接種事業の対象者
⑥提供方法	[<input checked="" type="checkbox"/>] 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	情報提供ネットワークシステムを通じて依頼のあった都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

6. 特定個人情報の保管・消去

①保管場所 ※		<p><事務室における措置> 町田市情報セキュリティポリシーにより規定 ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。</p> <p><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いる。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。</p> <p><ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。</p> <p><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。</p>
	②保管期間	<p>期間</p> <p>[5年]</p> <p>その妥当性</p>

<p>③ 消去方法</p>	<p>・データベースに記録されたデータのうち、法定保存年限を経過したデータをシステムから消去する。</p> <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破砕、溶解、焼却等の情報の復元不能化処理を行っている。 <p><中間サーバー・プラットフォームにおける措置></p> <ol style="list-style-type: none"> 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、物理的破壊または専用ソフト等を利用して完全に消去する。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p> <p><ガバメントクラウドにおける措置></p> <ol style="list-style-type: none"> 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等にしながら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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。
<p>7. 備考</p>	

番号法第9条第1項 別表1に定める行政事務を処理する者

別表第1のうち、事務に予防接種情報が含まれるものを抜粋

項番	項番 (別表1)	行政事務を処理する者	事務
1	10	十 都道府県知事又は市町村長	予防接種法(昭和二十三年法律第六十八号)による予防接種の実施、給付の支給又は実費の徴収に関する事務であつて主務省令で定めるもの
2	93の2	九十三の二 厚生労働大臣、都道府県知事又は市町村長	新型インフルエンザ等対策特別措置法(平成二十四年法律第三十一号)による予防接種の実施に関する事務であつて主務省令で定めるもの

番号法第19条第8号別表2に定める情報照会者

別表第2のうち、特定個人情報に予防接種関係情報が含まれるものを抜粋

項番	項番 (別表2)	情報照会者	事務	情報提供者	特定個人情報
1	16の2	十六の二 市町村長	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの	都道府県知事又は市町村長	予防接種法による予防接種の実施に関する情報であって主務省令で定めるもの
2	17	十七 市町村長	予防接種法による給付(同法第十五条第一項の疾病に係るものに限る。)の支給に関する事務であって主務省令で定めるもの	医療保険者その他の法令による医療に関する給付の支給を行うこととされている者	医療保険各法その他の法令による医療に関する給付の支給に関する情報であって主務省令で定めるもの
3	18	十八 市町村長	予防接種法による給付の支給又は実費の徴収に関する事務であって主務省令で定めるもの	市町村長	地方税関係情報又は住民票関係情報であって主務省令で定めるもの
4	19	十九 市町村長	予防接種法による給付(同法第十五条第一項の障害に係るものに限る。)の支給に関する事務であって主務省令で定めるもの	特別児童扶養手当等の支給に関する法律その他の法令による障害を有する者について支給される手当を支給することとされている者	特別児童扶養手当等の支給に関する法律その他の法令による障害を有する者に対する手当の支給に関する情報であって主務省令で定めるもの
5	115の2	百十五の二 市町村長	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの	厚生労働大臣、都道府県知事又は市町村長	新型インフルエンザ等対策特別措置法による予防接種の実施に関する情報であって主務省令で定めるもの

(別添2) 特定個人情報ファイル記録項目

別紙「個人情報ファイル簿」とおり

個人情報ファイル簿

2024年5月27日時点

1	個人情報ファイルの名称	予防接種	備考
2	行政機関の名称	町田市	
3	個人情報ファイルが利用に供される事務をつかさどる組織の名称	保健所保健予防課	
4	個人情報ファイルの利用目的	伝染病の予防とまん延の防止 その他詳細は別紙のとおり	
5	(1) 基本的項目 氏名	○	
5	(1) 基本的項目 個人番号	○	個人番号収集の際の本人確認に使用する情報を含む。
5	(1) 基本的項目 住所	○	
5	(1) 基本的項目 性別	○	
5	(1) 基本的項目 生年月日	○	予防接種対象者、保護者、親族及び健康被害対象者のみ。
5	(1) 基本的項目 電話番号	○	
5	(1) 基本的項目 本籍		
5	(1) 基本的項目 国籍	○	
5	(1) 基本的項目 世帯主との続柄		
5	(1) 基本的項目 親族関係		
5	(1) 基本的項目 家庭環境等	○	
5	(1) 基本的項目 人種※		
5	(1) 基本的項目 社会的身分※		
5	(1) 基本的項目 電子メールアドレス	○	予防接種スケジュールに関する電子メールの配信希望者、小児の優先接種希望者のみ。
5	(1) 基本的項目 住民異動年月日	○	予防接種対象者、保護者、親族及び健康被害対象者のみ。
5	(1) 基本的項目 死亡	○	
5	(1) 基本的項目 住民記録システム注意情報	○	
5	(1) 基本的項目 渡航歴	○	渡航に伴い接種歴を証明する必要があるため。
5	(1) 基本的項目 保護者	○	
5	(2) 思想・信条等に関する項目 主義・主張※		
5	(2) 思想・信条等に関する項目 支持政党		
5	(2) 思想・信条等に関する項目 宗教※		
5	(2) 思想・信条等に関する項目 趣味・嗜好		
5	(3) 社会的地位等に関する項目 職業・職歴	○	予防接種対象者及びその保護者、親族のみ。
5	(3) 社会的地位等に関する項目 地位		
5	(3) 社会的地位等に関する項目 学歴		
5	(3) 社会的地位等に関する項目 各種団体加入		
5	(3) 社会的地位等に関する項目 賞罰		
5	(3) 社会的地位等に関する項目 犯歴※		
5	(3) 社会的地位等に関する項目 利用施設名	○	
5	(4) 成績・資格等に関する項目 学業成績		
5	(4) 成績・資格等に関する項目 勤務成績		
5	(4) 成績・資格等に関する項目 各種試験成績		
5	(4) 成績・資格等に関する項目 各種資格		
5	(5) 財産・収入に関する項目 収入状況		
5	(5) 財産・収入に関する項目 財産状況		
5	(5) 財産・収入に関する項目 納税額等	○	予防接種対象者及びその保護者、親族のみ。
5	(5) 財産・収入に関する項目 取引状況		
5	(5) 財産・収入に関する項目 公的扶助の受給	○	予防接種対象者及びその保護者、親族のみ。
5	(5) 財産・収入に関する項目 各種貸付金		
5	(5) 財産・収入に関する項目 住居の間取り・図面		
5	(5) 財産・収入に関する項目 金融機関名	○	健康被害関係者、予防接種対象者及びその保護者、親族のみ。
5	(5) 財産・収入に関する項目 口座番号	○	健康被害関係者、予防接種対象者及びその保護者、親族のみ。
5	(5) 財産・収入に関する項目 犯罪被害※		
5	(5) 財産・収入に関する項目 助成金	○	予防接種対象者及びその保護者、親族のみ。
5	(5) 財産・収入に関する項目 被災	○	東日本大震災で被災し、市内に避難してこられた方のみ。
5	(5) 財産・収入に関する項目 示談の内容	○	
5	(6) 心身等に関する項目 健康状況	○	予防接種対象者、保護者、親族及び健康被害対象者、予防接種助成対象者のみ。
5	(6) 心身等に関する項目 障がいの状況※	○	予防接種対象者、保護者、親族及び健康被害対象者、予防接種助成対象者のみ。
5	(6) 心身等に関する項目 容姿（写真）		
5	(6) 心身等に関する項目 健診・検査※		

5	(6) 心身等に関する項目 病名※	○	予防接種対象者、保護者、親族及び健康被害対象者、予防接種助成対象者のみ。
5	(6) 心身等に関する項目 診療・調剤※		
5	(6) 心身等に関する項目 犯罪被害※		
5	(6) 心身等に関する項目 予防接種歴	○	予防接種対象者、保護者、親族及び健康被害対象者、予防接種助成対象者のみ。
5	(6) 心身等に関する項目 医療機関名	○	予防接種対象者、保護者、親族及び健康被害対象者、予防接種助成対象者のみ。
5	(6) 心身等に関する項目 妊娠	○	予防接種対象者のみ。
5	(6) 心身等に関する項目 事故(けが)の状況	○	予防接種事故損害賠償補償対応時のみ。
5	(6) 心身等に関する項目 死亡の原因	○	予防接種事故損害賠償補償対応時のみ。
6	記録範囲	① 予防接種対象者及びその保護者、親族 ② ①の内、予防接種助成対象者 ③ 予防接種関係医師 ④ 予防接種健康被害関係者 ⑤ 東日本大震災で被災し、市内に避難してこられた被災者 ⑥ 成年後見人	
7	記録情報の収集方法	文書(紙)・電子媒体(データ)	
8	要配慮個人情報が含まれるときは、その旨	○	
9	記録情報の経常的提供先	別紙のとおり	
10	開示請求等を受理する組織の名称及び所在地	保健所保健予防課(町田市森野2-2-22)	
11	訂正及び利用停止に関する他の法律又はこれに基づく命令の規定による特別の手續等		
12	個人情報ファイルの種別: 法第60条第2項第1号(電算処理ファイル)	○	
12	個人情報ファイルの種別: (電算処理ファイルの場合) 令第21条第7項に該当するファイル(電算処理ファイルに付随するマニュアル処理ファイル)の有無	有	
12	個人情報ファイルの種別: 法第60条第2項第2号(マニュアル処理ファイル)		
13	行政機関等匿名加工情報の提案の募集をする個人情報ファイルである旨	実施しない	
14	行政機関等匿名加工情報の提案を受ける組織の名称及び所在地	実施しない	
15	行政機関等匿名加工情報の概要	実施しない	
16	作成された行政機関等匿名加工情報に関する提案を受ける組織の名称及び所在地	実施しない	
17	作成された行政機関等匿名加工情報に関する提案をすることができる期間	実施しない	
18	記録情報に条例要配慮個人情報が含まれているときはその旨	なし	
19	備考		

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

予防接種対象者関係情報ファイル

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

<p>対象者以外の情報の入手を防止するための措置の内容</p>	<p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・業務上、必要のない情報資産を作成しない。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・情報資産は適切に保管している。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <ul style="list-style-type: none"> ・当市の転入者について、転出元市区町村へ接種記録を照会するために、本人から個人番号を入手する場合は、接種券発行申請書兼接種記録同意確認書等により本人同意を取得し、さらに番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ・当市からの転出者について、当市での接種記録を転出先市区町村へ提供するために、他市区町村から個人番号を入手するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。 ・当市への転入者について、転出元市区町村から接種記録を入手するが、その際は、当市において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入手するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 <p>(新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付)</p> <p>交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。</p>
<p>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</p>	<p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・業務上、必要のない情報資産を作成しない。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・情報資産は適切に保管している。 <p><ワクチン接種記録システム等における追加措置></p> <p>(新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付)</p> <ul style="list-style-type: none"> ・個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。
<p>その他の措置の内容</p>	<ul style="list-style-type: none"> ・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。
<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

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	<ul style="list-style-type: none"> 紙の申請書類等、本人等を通じて入手する場合は、説明書等を用いて利用目的を本人に明示する。 予防接種台帳システムを利用する職員を限定し、個人ごとにユーザーID及びパスワードを発行し、端末利用時は画像認証を行っている。また、利用者権限を設定することによって、認証後に入手可能な情報に制限をかける。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ワクチン接種記録システム(VRS)のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	<ul style="list-style-type: none"> 番号法第16条に基づいた本人確認の措置を行う。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが送信される。
個人番号の真正性確認の措置の内容	<ul style="list-style-type: none"> 本人が持参する個人番号カードで確認する。 住民基本台帳ネットワークで確認する。 転入前住所等の市町村に照会する。
特定個人情報の正確性確保の措置の内容	<ul style="list-style-type: none"> 入力、削除及び訂正作業に用いた帳票等は、当市で定める規程に基づいて管理、保管又は廃棄する。 登録された特定個人情報は、アクセス権限を設定し厳しい制限をかけ、ログ管理を実施する。変更があった場合には、異動リスト等により確認ができる。 <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> 業務上、必要のない情報資産を作成しない。 不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 システムや端末利用者を識別するアカウントの管理を行う。 アカウントのアクセス権限は、必要最小限度の設定としている。 異動等により、不要となったアカウントについては削除している。 管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 情報資産は適切に保管している。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 券面入力補助APを活用し、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情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。
その他の措置の内容	<ul style="list-style-type: none"> 端末のアクセス制御を実施するためICカードシステムを導入している。 IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 IDとパスワードによるアクセス制御を実施できるシステムを導入している。 権限管理が実施できるシステムを導入している。
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・特定個人情報を回線を通じて入手する場合は、他のシステムからのアクセスが行えない専用回線を用いることにより、情報漏えい防止措置を講じる。 ・申告書等の取扱いについては手順化され運用している。 <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットにて保管し、退庁時に施錠している。 ・端末については、盗難防止具（鍵付チェーン等）の使用または鍵付キャビネットへの保管を行っている。 ・業務上、必要のない情報資産を作成しない。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時には、一般権限のアカウントを利用している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 ・相談室には個室又はパーテーションを設置している。 <p><ワクチン接種記録システム（VRS）における追加措置></p> <ul style="list-style-type: none"> ・入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 <p>（新型コロナウイルス感染症予防接種証明書電子交付機能）</p> <ul style="list-style-type: none"> ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 <p>（新型コロナウイルス感染症予防接種証明書コンビニ交付）</p> <ul style="list-style-type: none"> ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	
<ul style="list-style-type: none"> ・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。 <p>派遣労働者については派遣契約約款により以下を規定</p> <ul style="list-style-type: none"> ・派遣元は派遣業務の遂行により知り得た個人情報を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。 ・機密保持義務履行の誓約書の提出を派遣元に求めることができる。 <p><ワクチン接種記録システム（VRS）における追加措置></p> <ul style="list-style-type: none"> ・入手した特定個人情報については、限定された端末を利用して本市が指定する管理者から配布されたユーザーIDを使用し、ログインした場合だけアクセスできるように制御している。 	

3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な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	<ul style="list-style-type: none"> ・宛名システム等における個人番号を番号法及び条例上認められないシステムと紐付けできないように制御する。 ・個人番号利用業務以外の業務では、個人番号が含まれない画面表示とする。 ・個人番号利用業務以外の業務から予防接種情報の要求があった場合は、個人番号が含まれない情報のみを提供し、個人番号には一切アクセスできないようアクセス制御を行う。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・接種会場等では、接種券番号の読取端末(タブレット端末)からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないよう制御している。
事務で使用するその他のシステムにおける措置の内容	「3. 特定個人情報の使用 リスク1: 目的を超えた紐付け、事務に必要な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」と同じ。
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
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> 1) 行っている 2) 行っていない
具体的な管理方法	<p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>権限のない者によって不正に使用されないよう、以下の対策を講じている。</p> <ul style="list-style-type: none"> ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LG-WAN端末による操作に限り可能になるよう制御している。 ・LG-WAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用ユーザIDは、当市が指定する管理者が認めた者に限定して発行される。
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	<p>「3. 特定個人情報の使用 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 具体的な管理方法」と同じ。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、当市が指定する管理者が必要最小限の権限で発効する。</p> <p>当市が指定する管理者は、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。</p> <p>やむを得ず、複数の職員が共有するID(以下「共用ID」という。)を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動/退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。</p>

アクセス権限の管理	<input type="checkbox"/> 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	「3. 特定個人情報の使用 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)によつて不正に使用されるリスク ユーザ認証の管理 具体的な管理方法」と同じ。
特定個人情報の使用の記録	<input type="checkbox"/> 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	町田市情報セキュリティポリシーにより規定 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 <ワクチン接種記録システム(VRS)における追加措置> ・システム上の操作のログを取得しており、操作ログを確認できる。ログは定期に及び必要に応じ随時に確認する。
その他の措置の内容	・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。 派遣労働者については派遣契約約款により以下を規定 ・派遣元は派遣業務の遂行により知り得た個人情報を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。 ・機密保持義務履行の誓約書の提出を派遣元に求めることができる。
リスクへの対策は十分か	<input type="checkbox"/> 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

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	<p>町田市情報セキュリティポリシーにより規定</p> <p><事務室における措置></p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <p><アクセス制御></p> <ul style="list-style-type: none"> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等。 <p><その他の措置></p> <ul style="list-style-type: none"> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。 <p>派遣労働者については派遣契約約款により以下を規定</p> <ul style="list-style-type: none"> ・派遣元は派遣業務の遂行により知り得た個人情報を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。 ・機密保持義務履行の誓約書の提出を派遣元に求めることができる。
リスクへの対策は十分か	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

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	「3. 特定個人情報の使用 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」と同じ。
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	
<ul style="list-style-type: none"> ・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。 <p><ワクチン接種記録システム(VRS)における追加措置> 特定個人情報を使用する場面を必要最小限に限定している。具体的には、以下の3つの場面に限定している。</p> <ul style="list-style-type: none"> ・当市への転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・当市からの転出者について、当市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 <p>また、ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。</p>	

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

- ・ISO/IEC27001 (ISMS)の認証を受けていることを業者選定の際の条件としている。
- ・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。
- ・委託先は原則的に特定個人情報ファイルを取り扱わない。
- ・委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。

<新型コロナウイルス感染症対策に係る予防接種事務における追加措置>
 当市区町村、国、当該システムの運用保守事業者の三者の関係の規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。

- ・特定個人情報ファイルの閲覧者・更新者の制限
- ・特定個人情報ファイルの取扱いの記録
- ・特定個人情報の提供ルール/消去ルール
- ・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
- ・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
- ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置

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

- ・作業者を限定するために、委託にかかる実施体制の提出を義務付けている。
- ・委託先は原則的に特定個人情報ファイルを取り扱わない。

町田市情報セキュリティポリシーにより規定

- ・システムや端末利用者を識別するアカウントの管理を行う。
- ・アカウントのアクセス権限は、必要最小限度の設定としている。
- ・異動等により、不要となったアカウントについては削除している。
- ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。
- ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。

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>
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

- ・委託業務の実施状況について定期的に報告を受けるとともに、その記録を残している。
- ・委託先は原則的に特定個人情報ファイルを取り扱わない。

町田市情報セキュリティポリシーにより規定

- ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。

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内容及びルール遵守の確認方法

委託先から他者へ提供することはない。

	<p>委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法</p>	<ul style="list-style-type: none"> ・委託先へ原則的に提供することはない。 <p>提供する場合は次のとおり。</p> <p>磁気データの管理と取扱いに関する要領により規定</p> <ul style="list-style-type: none"> ・受渡しは、受渡確認書(別記様式)により確認し、行っている。 ・受渡しは、コンピュータセンター内の決められた場所で行っている。
<p>特定個人情報の消去ルール</p>	<p>[定めている]</p>	<p><選択肢> 1) 定めている 2) 定めていない</p>
	<p>ルール内容及びルール遵守の確認方法</p>	<ul style="list-style-type: none"> ・原則的に特定個人情報を含むデータの消去の委託はしない。 ・消去した旨の書面を提出させる。 <p>情報セキュリティ確保・個人情報保護のための特記仕様書により規定</p> <ul style="list-style-type: none"> ・契約の終了後又は解除後、委託先は、市に返還又は納入する物もしくは特に保管を要する物を除き、受託業務の実施にあたり作成した情報の一切を抹消、焼却、切断その他の方法により復元不可能な状態にして処分するものとしている。
<p>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</p>	<p>[定めている]</p>	<p><選択肢> 1) 定めている 2) 定めていない</p>
<p>規定の内容</p>	<p>委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。</p>	
<p>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</p>	<p>[十分に行っている]</p>	<p><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</p>
<p>具体的な方法</p>	<p>「4. 特定個人情報ファイルの取扱いの委託 委託契約中の特定個人情報ファイルの取扱いに関する規定 規定の内容」と同じ。</p>	
<p>その他の措置の内容</p>	<p>—</p>	
<p>リスクへの対策は十分か</p>	<p>[十分である]</p>	<p><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</p>
<p>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</p>		
<p>—</p>		

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	<p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> 不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供等の記録」を入手し、記録の確認をすることができる。</p>	
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
ルール内容及びルール遵守の確認方法	<ul style="list-style-type: none"> 番号法及び条例上認められる場合のみ提供及び移転を行う。 番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 <p>磁気データの管理と取扱いに関する要領により規定</p> <p>第5 磁気データの利用</p> <ol style="list-style-type: none"> 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。 	
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
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	<ul style="list-style-type: none"> 番号法及び条例上認められる場合のみ提供及び移転を行う。 番号法及び条例上認められる提供及び移転以外に、提供・移転する機能をシステム上設けない。 <p>磁気データの管理と取扱いに関する要領により規定</p> <p>第5 磁気データの利用</p> <ol style="list-style-type: none"> 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課（以下「データ利用課」という。）の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。 <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> 不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 情報セキュリティ内部監査員を養成するための教育をしている。 <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <ul style="list-style-type: none"> 他市区町村への個人番号の提供 <p>当市区町村への転入者について、転出元市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を用いて提供する。</p> <p>転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン</p>	
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

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	<p>・統合連携基盤では、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。</p> <p>・統合連携基盤では、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。</p> <p><中間サーバー・ソフトウェアにおける措置></p> <p>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、提供許可証の発行と照会内容の照会許可照会リスト(※2)との照会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。</p> <p>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。</p> <p>(※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。</p> <p>(※2) 番号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。</p> <p>(※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。</p>		
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 3) 課題が残されている	2) 十分である
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	<p>・統合連携基盤では、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。</p> <p>・統合連携基盤では、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。</p> <p><中間サーバー・ソフトウェアにおける措置></p> <p>①中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・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。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p>		
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 3) 課題が残されている	2) 十分である
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	<p>・統合連携基盤では、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。</p> <p>・統合連携基盤では、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。</p>		
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 3) 課題が残されている	2) 十分である

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	<p>・統合連携基盤では、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。</p> <p>・統合連携基盤では、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。</p> <p><中間サーバー・ソフトウェアにおける措置></p> <p>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(※)。</p> <p>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。</p> <p>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、一定期間経過後に結果情報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。</p> <p>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。</p> <p>(※)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。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>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。</p> <p>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ない。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>
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	<p>・統合連携基盤では、情報の提供について、連携時のアクセスログと連携データが特定できるよう記録している。</p> <p>・統合連携基盤では、番号法及び条例上認められる提供以外に、提供する機能をシステム上設けない。</p> <p><中間サーバー・ソフトウェアにおける措置></p> <p>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照会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、照会許可照会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。</p> <p>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。</p> <p>③機微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。</p> <p>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。</p> <p>(※)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。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

<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	[十分に遵守している]	<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	[十分に整備している]	<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	[十分に整備している]	<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	[十分に周知している]	<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	[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

具体的な対策の内容	<p>町田市情報セキュリティポリシーにより規定</p> <p><事務室における措置></p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>②事前に申請し承認されてない物品、記憶媒体、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。</p> <p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。</p> <p>主に以下の物理的対策を講じている。</p> <ul style="list-style-type: none"> ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 <p><ガバメントクラウドにおける措置></p> <p>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。</p> <p>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。</p>
-----------	---

<p>⑥技術的対策</p> <p>具体的な対策の内容</p>	<p>[十分に行っている] <選択肢></p> <p>1) 特に力を入れて行っている 2) 十分に行っている</p> <p>3) 十分に行っていない</p>
	<p>端末は記録媒体が接続できない仕様になっている。</p> <ul style="list-style-type: none"> ・端末はインターネット接続ができない仕様になっている。 ・特定個人情報を回線により入手する場合は、他のシステムからのアクセスが行えない専用回線を用いている。 <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・ウイルス対策ソフトを導入している。 ・ウイルス対策の対象は、サーバ、クライアント(端末)及びゲートウェイを含めた、包括的な対策を講じている。 ・常に最新のウイルス定義ファイル(パターンファイル)を使用している。 ・定期的にウイルス対策の実施状況を確認している。 ・インターネット等外部ネットワークとは分離し、不正アクセス防止をしている。 ・外部接続(インターネット接続を含む)におけるアクセス制御に関する管理策として、ファイアウォールやルータを設置している。 ・ハードウェア及びソフトウェアには、セキュリティ修正プログラムを適用している。 ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト(ログオフ)、画面表示を起動初期状態(情報の検索結果などが表示されていない状態)にする等 <p><中間サーバー・プラットフォームにおける措置></p> <ol style="list-style-type: none"> 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。 <p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。</p> <p>主に以下の技術的対策を講じている。</p> <ul style="list-style-type: none"> ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 <p>(新型コロナウイルス感染症予防接種証明書電子交付機能)</p> <ul style="list-style-type: none"> ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 <p>(新型コロナウイルス感染症予防接種証明書コンビニ交付)</p> <ul style="list-style-type: none"> ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 <p>また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。</p> <p><ガバメントクラウドにおける措置></p> <ol style="list-style-type: none"> 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。 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。 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

⑦バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
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	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
その内容	-	
再発防止策の内容	-	
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	死者の特定個人情報は、生存する個人の特定個人情報と分けて管理していないため、「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」において示す、生存する個人の特定個人情報ファイルと同様の管理を行う。	
その他の措置の内容	<ul style="list-style-type: none"> ・端末のアクセス制御を実施するためICカードシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できる端末認証の仕組みを導入している。 ・端末に情報を残さない仕組みであるシンクライアントシステムを導入している。 ・IDとパスワードによるアクセス制御を実施できるシステムを導入している。 ・権限管理が実施できるシステムを導入している。 <p>派遣労働者については派遣契約約款により以下を規定</p> <ul style="list-style-type: none"> ・派遣元は派遣業務の遂行により知り得た個人情報を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。 ・機密保持義務履行の誓約書の提出を派遣元に求めることができる。 	
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

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	個人番号を含め宛名情報については、住民基本台帳システムより随時異動データを連携することにより、最新化する。
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
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	<ul style="list-style-type: none"> ・保管期間の過ぎた特定個人情報は、予防接種事務に必要なか否かを判別したうえ消去する。 ・消去処理の実施後、抹消されていることを確認する。 ・磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。 ・紙媒体は保管期間ごとに分けて保管し、保管期間が過ぎているものについて外部業者による裁断溶解処理を行う。 <p>町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。 ・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。 ・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。 <p><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。</p>
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	<p>[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</p>
具体的なチェック方法	<p>情報セキュリティポリシーに基づく内部監査の一環で、チェックリストにて自己点検を全庁にわたり毎年度実施する。</p> <p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p>
②監査	<p>[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</p>
具体的な内容	<p>町田市情報セキュリティポリシーにより規定 ・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。</p> <p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p> <p><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。</p>

2. 従業者に対する教育・啓発

従業者に対する教育・啓発	<p style="text-align: center;">[十分に行っている]</p> <p style="text-align: right;"><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</p>
具体的な方法	<ul style="list-style-type: none"> ・派遣労働者に対して、セキュリティポリシーの理解と遵守及び情報システムの適正な運用を行うことを目的とする教育を行う。 町田市情報セキュリティポリシーにより規定 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 <p><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料を作成し、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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。</p>

3. その他のリスク対策

	<p><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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> 厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。</p> <p><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。</p>
--	---

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194-8520 東京都町田市森野2-2-22 担当課:総務部 法務課 電話:042-724-8407FAX:050-3085-3142
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。また、請求方法について、ホームページにおいて要領を記載し、わかりやすい説明に努めている。
特記事項	市ホームページ上に、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	予防接種ファイル
公表場所	総務部法務課
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	郵便番号194-8520 東京都町田市森野2-2-22 担当課:保健所保健予防課保健予防係 電話:042-725-5422(保健予防課保健予防係) FAX:050-3161-8634
②対応方法	窓口・電話・FAX等による。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和6年7月1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] <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	意見公募の実施について、町田市ホームページに掲載し、同ホームページ、市庁舎、市民センター、駅前連絡所等にて全文を閲覧できるようにする。意見聴取の方法は、郵便、FAX、電子メール及び事務担当課への持参による。
②実施日・期間	令和6年5月15日から令和6年6月15日まで
③期間を短縮する特段の理由	
④主な意見の内容	評価書に対する意見は寄せられなかった。
⑤評価書への反映	
3. 第三者点検	
①実施日	令和6年6月21日
②方法	株式会社NTTデータに委託し、点検を行った。
③結果	下記の内容について修正の検討を前提として、適合性・妥当性の観点から問題ないとの点検結果を得た。 ・「Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所」、「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 3. 特定個人情報の使用 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」、「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. 特定個人情報の保管・消去 ⑤物理的対策 具体的な対策の内容」最初の箇所(Ⅱ 特定個人情報ファイルの概要 - 6. 特定個人情報の保管・消去 - ①保管場所)の「事務室における措置」では、「端末については、盗難防止具(鍵付きチェーン等)を使用している。」と記載されています。一方、これ以降の箇所の「事務室における措置」では、「端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。」と記載されています。これらが同じ事務室を指している場合、同様の対策が実施されているものと考えられます。確認の上、必要に応じ、内容を統一するなどの修正をお願いいたします。
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
令和5年3月15日	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	(追加)	4. 給付の支給(予防接種法に基づく予防接種の場合) ①健康被害が生じた場合、住民(被害者)から健康被害の給付申請を受理 ②申請内容を本市で審議した後、申請書類等を国へ進達 ③健康被害が認定された場合は、被害者に対して給付金を支給 5. 給付の支給(予防接種法に基づかない予防接種の場合) ①健康被害が生じた場合、町田市予防接種事故災害補償規則に基づき、住民(被害者)に対して、補償金等を支給 6. 接種券の作成 年齢・性別・個人接種歴から、必要な予防接種の接種券を作成 7. 予防接種証明書の作成 個人接種歴を使用して、予防接種証明書を出力 8. 各種統計の作成 各種統計を作成	事前	
令和5年3月15日	I 基本情報 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2 ②システムの機能	(追加)	6. 新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 7. 新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施	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
令和5年3月15日	I 基本情報 5. 個人番号の利用 法令上の根拠	(追加)	・第19条第6号(委託先への提供)	事後	
令和5年3月15日	新型コロナ接種模式図	(追加)	コンビニ等を通じた接種証明書交付の追加	事後	
令和5年3月15日	II 特定個人情報ファイルの 概要 3. 特定個人情報の入手・使用 ③入手に係る妥当性	・新型コロナウイルス感染症対策に係る予防接種事務においては、本市への転入者について、転出元自治体へ接種記録を照会するために、転入者本人から個人番号の提供の同意が得られた場合のみ入手する。(番号法第19条第15号) ・新型コロナウイルス感染症対策に係る予防接種事務においては、本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために、転出先市区町村から個人番号を入手する。(番号法第19条第15号)	・新型コロナウイルス感染症対策に係る予防接種事務においては、本市への転入者について、転出元市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。(番号法第19条第16号) ・新型コロナウイルス感染症対策に係る予防接種事務においては、本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために、他市区町村から個人番号を入手する。(番号法第19条第16号)	事後	
令和5年3月15日	II 特定個人情報ファイルの 概要 3. 特定個人情報の入手・使用 ⑤本人への明示	(追加)	・電子交付アプリにより、予防接種証明書の電子申請を受ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受ける場合においては、利用規約を表示し、同意を得てから入手する。	事後	
令和5年3月15日	II 特定個人情報ファイルの 概要 3. 特定個人情報の入手・使用 ⑧使用方法	(追加)	・申請書で公金受取口座での受取希望(同意)があった場合、情報提供ネットワークシステムから公金受取口座情報を取得し、申請書の口座情報欄に転記する。	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
令和5年3月15日	II 特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ⑧使用方法 情報の突合	(転出先市区町村にて、本人から個人番号の提供に関して同意が得られた場合のみ等処理を行う。)	(削除)	事後	
令和5年3月15日	II 特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 委託事項1	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	事後	
令和5年3月15日	II 特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 ①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	事後	
令和5年3月15日	II 特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	
令和5年3月15日	II 特定個人情報ファイルの概要 4.特定個人情報ファイルの取扱いの委託 ④委託先への特定個人情報ファイルの提供方法	[O] その他 LG-WAN回線を用いた提供	[O] その他 LG-WAN回線を用いた提供(VRS本体、コンビニ交付関連機能)、本人からの電子交付アプリを用いた提供(新型コロナウイルス感染症予防接種証明書電子交付機能)	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
令和5年3月15日	II 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ① 保管場所	(追加)	<p><ワクチン接種記録システム(VRS)における追加措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。</p> <ul style="list-style-type: none"> ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 <p>(新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。</p> <p>(新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。</p>	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
令和5年3月15日	II 特定個人情報ファイルの概要 6.特定個人情報の保管・消去 ③消去方法	(追加)	<p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。 ・自機関の領域に保管されたデータは、他機関から消去できない。 <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p>	事後	
令和5年3月15日	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 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。) 対象者以外の情報の入手を防止するための措置の内容	(追加)	<p>(新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付)</p> <p>交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。</p>	事後	
令和5年3月15日	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 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。) 必要な情報を入手することを防止するための措置の内容	(追加)	<p><ワクチン接種記録システム等における追加措置></p> <p>(新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付)</p> <ul style="list-style-type: none"> ・個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。 	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
令和5年3月15日	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 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2 リスクに対する措置の内容	(追加)	(新型コロナウイルス感染症予防接種証明書電 子交付機能) ・当該機能では、専用アプリからのみ交付申請 を可能とする。アプリの改ざん防止措置を講じる ことで、意図しない不適切な方法で特定個人情 報が送信されることを避ける。 (新型コロナウイルス感染症予防接種証明書コ ンビニ交付) ・証明書交付センターにおいてキオスク端末の 操作画面を制御し、コンビニ交付に対応する市 町村に対してのみキオスク端末から交付申請を 可能とすることで、意図しない不適切な方法で 特定個人情報が送信されることを避ける。	事後	
令和5年3月15日	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 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。) 入手の際の本人確認の措置 の内容	(追加)	<ワクチン接種記録システム(VRS)における追 加措置> (新型コロナウイルス感染症予防接種証明書電 子交付機能、コンビニ交付) ・個人番号カードのICチップ読み取り(券面事項 入力補助AP)と暗証番号入力(券面事項入力補 助APの暗証番号)による二要素認証で本人確 認を行うため、本人からの情報のみが送信され 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
令和5年3月15日	<p>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</p> <p>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。)</p> <p>特定個人情報の正確性確保の措置の内容</p>	(追加)	<p><ワクチン接種記録システム(VRS)における追加措置></p> <p>(新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付)</p> <ul style="list-style-type: none"> ・券面入力補助APを活用し、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情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。 	事後	
令和5年3月15日	<p>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</p> <p>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。)</p> <p>リスク4</p> <p>リスクに対する措置の内容</p>	(追加)	<p>(新型コロナウイルス感染症予防接種証明書電子交付機能)</p> <ul style="list-style-type: none"> ・電子交付アプリとVRSとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 <p>(新型コロナウイルス感染症予防接種証明書コンビニ交付)</p> <ul style="list-style-type: none"> ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 <p>また、通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。</p> <p>さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。</p>	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
令和5年3月15日	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 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。) 特定個人情報の入手(情報提 供ネットワークを通じた入手を 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	・入手した特定個人情報については、限定され た端末を利用して国から皮膚されたユーザーID を使用し、ログインした場合だけアクセスできる ように制御している。	・入手した特定個人情報については、限定され た端末を利用して当市が指定する管理者から配 布されたユーザーIDを使用し、ログインした場合 だけアクセスできるように制御している。	事前	
令和5年3月15日	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 3. 特定個人情報の使用 リスク2 ユーザー認証の管理 具体的な管理方法	・ワクチン接種記録システム(VRS)へのログイン 用ユーザーIDは、国に対してユーザ登録を事前 申請した者に限定して発行される。	・ワクチン接種記録システム(VRS)へのログイン 用ユーザーIDは、当市が指定する管理者が認 めた者に限定して発行される。	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
令和5年3月15日	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 3.特定個人情報の使用 リスク2 アクセス権限の発行・失効の 管理 具体的な管理方法	(追加)	<ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、当市が指定する管理者が必要最小限の権限で発効する。 当市が指定する管理者は、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。 やむを得ず、複数の職員が共有するID(以下「共用ID」という。)を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動/退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	事前	
令和5年3月15日	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 3.特定個人情報の使用 リスク2 アクセス権限の管理 具体的な管理方法	(追加)	<ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、当市が指定する管理者が必要最小限の権限で発効する。 当市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。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。	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
令和5年3月15日	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 3. 特定個人情報の使用 リスク2 特定個人情報の使用の記録 具体的な管理方法	・システム上の操作のログを取得しており、操作 ログを確認できる。	・システム上の操作のログを取得しており、操作 ログを確認できる。ログは定期的に及び必要に応 じ随時に確認する。	事前	
令和5年3月15日	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 3. 特定個人情報の使用 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	・当市への転入者について、転出元市区町村へ 接種記録を照会するために、転入者から個人番 号の提供の同意が得られた場合のみ入手し、 使用する。	・当市への転入者について、転出元市区町村へ 接種記録を照会する場合のみ入手し、使用す 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
令和5年3月15日	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 4. 特定個人情報ファイルの取 扱いの委託 情報保護管理体制の確認	(追加)	<p>〈新型コロナウイルス感染症対策に係る予防接種事務における追加措置〉</p> <p>当市区町村、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。</p> <ul style="list-style-type: none"> ・ 特定個人情報ファイルの閲覧者・更新者の制限 ・ 特定個人情報ファイルの取扱いの記録 ・ 特定個人情報の提供ルール/消去ルール ・ 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 ・ 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 ・ 新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置 	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
令和5年3月15日	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 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 を通じた提供を除く。) リスク2 リスクに対する措置の内容	(追加)	<新型コロナウイルス感染症対策に係る予防接 種事務における追加措置> ・他市区町村への個人番号の提供 当市区町村への転入者について、転出元市区 町村から接種記録を入手するため、他市区町村 へ個人番号を提供するが、その際は、住民基本 台帳等により照会対象者の個人番号であること を確認した情報を、ワクチン接種記録システム (VRS)を用いて提供する。 転出先市区町村へ接種記録を提供するが、そ の際は、転出元市区町村において、住民基本台 帳等により照会対象者の個人番号であることを 確認し、当該個人番号に対応する個人の接種 記録のみをワクチン接種記録システム(VRS)を 用いて提供する。	事後	
令和5年3月15日	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 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 を通じた提供を除く。) リスク3 リスクに対する措置の内容	(追加)	<ワクチン接種記録システム(VRS)における追 加措置> ・転出元他市区町村への個人番号の提供、転 出先市区町村への接種記録の提供 当市区町村への転入者について、転出元市区 町村から接種記録を入手するため、他市区町村 へ個人番号を提供するが、電文を受ける市区町 村で、該当者がいない場合は、個人番号は保管 されず、これに対して接種記録は提供されない 仕組みとなっている。	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
令和5年3月15日	<p>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</p> <p>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を通じた提供を除く。） 特定個人情報の提供・移転（委託や情報提供ネットワーク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</p>	(追加)	<p><ワクチン接種記録システム(VRS)における追加措置></p> <ul style="list-style-type: none"> ・特定個人情報の提供は、限定された端末(LG-WAN端末)だけができるように制御している。 ・特定個人情報を提供する場面を必要最小限に限定している。 <p>具体的には、当市区町村への転入者について、転出元市区町村での接種記録を入手するために、他市区町村へ個人番号を提供する場面に限定している。</p>	事後	
令和5年3月15日	<p>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</p> <p>7.特定個人情報の保管・消去</p> <p>⑤物理的対策 具体的な対策の内容</p>	(追加)	<p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。</p> <p>主に以下の物理的対策を講じている。</p> <ul style="list-style-type: none"> ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 	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
令和5年3月15日	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. 特定個人情報の保管・消去 ⑤技術的対策 具体的な対策の内容	(追加)	<ワクチン接種記録システム(VRS)における措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の	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
令和5年3月15日	<p>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</p> <p>7. 特定個人情報の保管・消去 ⑤技術的対策 具体的な対策の内容</p>	(追加)	<p>(新型コロナウイルス感染症予防接種証明書電子 交付機能)</p> <ul style="list-style-type: none"> ・電子交付アプリには、申請情報を記録しない こととしている。 ・電子交付アプリとVRSとの通信は暗号化を行 うことにより、通信内容の秘匿及び盗聴防止の 対応をしている。 <p>(新型コロナウイルス感染症予防接種証明書コ ンビニ交付)</p> <ul style="list-style-type: none"> ・証明書交付センターシステム及びキオスク端 末には、申請情報・証明書データを記録しないこ ととしている。 ・キオスク端末と証明書交付センターシステム 間の通信については専用回線、証明書交付セ ンターシステムとVRS間の通信については LGWAN回線を使用し、情報漏えいを防止する。 また、通信は暗号化を行うことにより、通信 内容の秘匿及び盗聴防止の対応をしている。 	事後	
令和5年3月15日	<p>Ⅳ その他のリスク対策</p> <p>1. 監査 ①自己点検 具体的なチェック方法</p>	(追加)	<p><新型コロナウイルス感染症対策に係る予防接 種事務における追加措置></p> <p>デジタル庁(旧内閣官房情報通信技術(IT)総合 戦略室)から発出された「新型コロナウイルスワ クチン接種記録システムの利用にあたっての確 認事項」に同意のうえ、第9条(市区町村の責 任)に則し、適切に職員等の当該システムの利 用を管理し、必要な監督をする。</p>	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
令和5年3月15日	IV その他のリスク対策 1. 監査 ② 監査 具体的な内容	(追加)	<p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p>	事後	
令和5年3月15日	IV その他のリスク対策 2. 従業者に対する教育・啓発 具体的な内容	(追加)	<p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。</p>	事後	
令和5年3月15日	IV その他のリスク対策 3. その他のリスク対策	(追加)	<p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。</p>	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
令和6年7月1日	II 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	<p><コンピュータ室における措置> 町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(危機の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 <p>設備状況</p> <ul style="list-style-type: none"> ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 <p><事務室における措置> 町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付きチェーン等)を使用している。 	<p><事務室における措置> 町田市情報セキュリティポリシーにより規定</p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 <p><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いる。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。</p>	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
		<p><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いる。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。</p> <p><ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。</p>	<p><ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 （新型コロナウイルス感染症予防接種証明書電子交付機能） 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。</p>		

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
		<p>・日本国内にデータセンターが存在するクラウドサービスを利用している。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。</p>	<p><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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	<p>II 特定個人情報ファイルの概要</p> <p>6. 特定個人情報の保管・消去</p> <p>③消去方法</p>	<p>・データベースに記録されたデータのうち、法定保存年限を経過したデータをシステムから消去する。</p> <p>町田市情報セキュリティポリシーにより規定</p> <p>・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。</p> <p>・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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事業者が特定個人情報を消去することはない。</p> <p>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、物理的破壊または専用ソフト等を利用して完全に消去する。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。</p> <p>・自機関の領域に保管されたデータは、他機関から消去できない。</p> <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p>	<p>・データベースに記録されたデータのうち、法定保存年限を経過したデータをシステムから消去する。</p> <p>町田市情報セキュリティポリシーにより規定</p> <p>・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。</p> <p>・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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事業者が特定個人情報を消去することはない。</p> <p>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、物理的破壊または専用ソフト等を利用して完全に消去する。</p> <p><ワクチン接種記録システム(VRS)における追加措置></p> <p>・自機関の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)を用いて消去することができる。</p> <p>・自機関の領域に保管されたデータは、他機関から消去できない。</p> <p>※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。</p>	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
			<p><ガバメントクラウドにおける措置></p> <p>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。</p> <p>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。</p> <p>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。この移行に際しては、システム基盤運用事業者がデータ抽出及び利用しなくなった環境の消去等を実施し、開発事業者がクラウド環境へのデータ投入等を実施する。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	<p>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</p> <p>3. 特定個人情報の使用リスク3:従業者が事務外で使用するリスク</p> <p>リスクに対する措置の内容</p>	<p>町田市情報セキュリティポリシーにより規定</p> <p><コンピュータ室における措置></p> <ul style="list-style-type: none"> ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる等)を禁止している。 ・室内の撮影等を禁止している。 ・危険物等(機器の動作に影響を与えるおそれのある通信機器を含む)の持ち込みを禁止している。 <p>設備状況</p> <ul style="list-style-type: none"> ・施錠管理できるサーバラック、監視カメラ、冗長化電源設備、無停電電源装置、非常用電源、専用空調設備、消火設備等。 <p><事務室における措置></p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)を使用している。 	<p>町田市情報セキュリティポリシーにより規定</p> <p><事務室における措置></p> <ul style="list-style-type: none"> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室管理簿への記載や、来客者用名札の着用等により、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。 	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
		<p><アクセス制御></p> <ul style="list-style-type: none"> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 <p><その他の措置></p> <ul style="list-style-type: none"> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 	<p><アクセス制御></p> <ul style="list-style-type: none"> ・システムや端末利用者を識別するアカウントの管理を行う。 ・アカウントのアクセス権限は、必要最小限度の設定としている。 ・異動等により、不要となったアカウントについては削除している。 ・管理者権限アカウントは、必要最小限度の利用とし、通常運用時においては、一般権限のアカウントを利用している。 ・不正アクセス時の追跡、不正アクセスの事前対策を講じる手段として定期的にログを監視・保管している。 ・情報資産は適切に保管している。 ・端末は画面表示を覗き見不可能な場所に設置、または覗き見防止フィルターを設置している。 ・離席時は、次の適切な管理を行っている。パソコンの電源を切る、パスワード付スクリーンセーバー、パソコンのキーボードロック、ログアウト（ログオフ）、画面表示を起動初期状態（情報の検索結果などが表示されていない状態）にする等。 <p><その他の措置></p> <ul style="list-style-type: none"> ・委託に際しては、契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付している。 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 		

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
		<p>・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。</p> <p>・情報セキュリティ内部監査員を養成するための教育をしている。</p> <p>・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。</p> <p>派遣労働者については派遣契約約款により以下を規定</p> <p>・派遣元は派遣業務の遂行により知り得た個人情報等を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。</p> <p>・機密保持義務履行の誓約書の提出を派遣元に求めることができる。</p>	<p>・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。</p> <p>・情報セキュリティ内部監査員を養成するための教育をしている。</p> <p>・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行う。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施する。</p> <p>派遣労働者については派遣契約約款により以下を規定</p> <p>・派遣元は派遣業務の遂行により知り得た個人情報等を第三者に漏えいしないものとし、これを派遣労働者に遵守・徹底させることとしている。また、契約終了後においても同様としている。</p> <p>・機密保持義務履行の誓約書の提出を派遣元に求めることができる。</p>		
令和6年7月1日	<p>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</p> <p>4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認</p>	<p>・委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。</p>	<p>・委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。</p>	事後	<p>個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更 に該当しない</p>

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6年7月1日	<p>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</p> <p>4. 特定個人情報ファイルの取扱いの委託 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 規定の内容</p>	<p>委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市個人情報保護条例、町田市セキュリティポリシーを遵守させている。</p>	<p>委託先には契約書に「情報セキュリティ確保・個人情報保護のための特記仕様書」を付し、町田市セキュリティポリシーを遵守させている。</p>	事後	<p>個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更 に該当しない</p>
令和6年7月1日	<p>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</p> <p>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。) 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・移転に関するルール ルール内容及びルール遵守の確認方法</p>	<p>磁気データの管理と取扱いに関する要領により規定</p> <p>第5 磁気データの利用</p> <p>1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課(以下「データ利用課」という。)の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。</p> <p>2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。</p> <p>3 前項の規定により、個人情報に係る処理を行うときは、町田市個人情報保護条例の規定を遵守しなければならない。</p> <p>町田市個人情報保護条例により規定(目的外利用、外部提供の制限)</p> <p>第13条 実施機関は、収集した保有個人情報について、第7条第1項の規定により登録された業務の目的の範囲を超えての利用(以下「目的外利用」という。)及び市の機関以外のものへの提供(以下「外部提供」という。)を行ってはならない。</p> <p>2 実施機関は、前項の規定にかかわらず、法令に特別の定めがある場合又は正当な職務執行に関連する場合で、審議会に諮問し、その答申に基づき行うときは、目的外利用又は外部提供を行うことができる。</p>	<p>磁気データの管理と取扱いに関する要領により規定</p> <p>第5 磁気データの利用</p> <p>1 磁気データの処理を新たに行い、又は変更するに当たり、他業務の磁気データを利用しようとする課(以下「データ利用課」という。)の情報管理者は、データ保有課の情報管理者に対し、磁気データの利用を申請して承諾を得なければならない。</p> <p>2 データ利用課の情報管理者は、前項の承諾を得た範囲内においてのみ、磁気データを利用できる。</p>	事後	<p>個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更 に該当しない</p>

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6年7月1日	<p>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</p> <p>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。)</p> <p>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</p>	<p>町田市個人情報保護条例により規定 (目的外利用、外部提供の制限)</p> <p>第13条 実施機関は、収集した保有個人情報に ついて、第7条第1項の規定により登録された業 務の目的の範囲を超えての利用(以下「目的外 利用」という。)及び市の機関以外のものへの提 供(以下「外部提供」という。)を行ってはならな い。</p> <p>2 実施機関は、前項の規定にかかわらず、法 令に特別の定めがある場合又は正当な職務執 行に関連する場合で、審議会に諮問し、その答 申に基づき行うときは、目的外利用又は外部提 供を行うことができる。</p>	(削除)	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
令和6年7月1日	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. 特定個人情報の保管・消 去 ⑤物理的対策 具体的な対策の内容	町田市情報セキュリティポリシーにより規定 <コンピュータ室における措置> ・施設案内を最小限の表示としている。 ・不正侵入者等の防止として、常時施錠し、必要 の都度、開閉している。 ・入退室者の登録管理を行っている。 ・入室者は、常時、名札を着用させている。 ・機器等への未承認のアクセス(操作、触れる 等)の禁止している。 ・室内の撮影等の禁止している。 ・危険物等(機器の動作に影響を与えるおそれ のある通信機器を含む)の持ち込み禁止してい る。 設備状況 ・施錠管理できるサーバラック、監視カメラ、冗 長化電源設備、無停電電源装置、非常用電源、 専用空調設備、消火設備等。 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室 管理簿への記載や、来客者用名札の着用等に より、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管 し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン 等)を使用している。	町田市情報セキュリティポリシーにより規定 <事務室における措置> ・関係者以外立ち入り禁止等を表示している。 ・職員については、名札を着用している。 ・来庁者の立ち入りを承認する場合は、入退室 管理簿への記載や、来客者用名札の着用等に より、入退管理をしている。 ・紙媒体については、鍵付きキャビネットで保管 し、退庁時に施錠している。 ・端末については、盗難防止具(鍵付チェーン 等)の使用または鍵付キャビネットへの保管を 行っている。 <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・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、記憶媒 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に、警備員などにより確認して 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
		<p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p>②事前に申請し承認されてない物品、記憶媒体、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に、警備員などにより確認している。</p> <p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。</p> <p>主に以下の物理的対策を講じている。</p> <ul style="list-style-type: none"> ・サーバー設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 	<p><ワクチン接種記録システム(VRS)における措置></p> <p>ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切な取扱いに関するガイドラインで求める物理的対策を満たしている。</p> <p>主に以下の物理的対策を講じている。</p> <ul style="list-style-type: none"> ・サーバー設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 <p><ガバメントクラウドにおける措置></p> <p>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。</p> <p>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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	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. 特定個人情報の保管・消 去 ⑥技術的対策 具体的な対策の内容	(末尾に右記文書追加)	<p>＜ガバメントクラウドにおける措置＞</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	<p>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</p> <p>7. 特定個人情報の保管・消去手順 手順の内容</p>	<p>・保管期間の過ぎた特定個人情報は、予防接種事務に必要なかを判別したうえ消去する。</p> <p>・消去処理の実施後、抹消されていることを確認する。</p> <p>・磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。</p> <p>・紙媒体は保管期間ごとに分けて保管し、保管期間が過ぎているものについて外部業者による裁断溶解処理を行う。</p> <p>町田市情報セキュリティポリシーにより規定</p> <p>・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。</p> <p>・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。</p> <p>・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。</p>	<p>・保管期間の過ぎた特定個人情報は、予防接種事務に必要なかを判別したうえ消去する。</p> <p>・消去処理の実施後、抹消されていることを確認する。</p> <p>・磁気ディスクの廃棄時は、規定に基づき、内容の復元及び判読が不可能になるような方法により消去する。</p> <p>・紙媒体は保管期間ごとに分けて保管し、保管期間が過ぎているものについて外部業者による裁断溶解処理を行う。</p> <p>町田市情報セキュリティポリシーにより規定</p> <p>・記録装置及び記録媒体は、物理的に破壊又はデータ復元不能化処理を行っている。</p> <p>・紙媒体は、シュレッダーによる破碎、溶解、焼却等の情報の復元不能化処理を行っている。</p> <p>・情報資産の廃棄時には、必要に応じ、廃棄日時、廃棄担当者、処理内容を記録している。</p> <p><ガバメントクラウドにおける措置></p> <p>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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	<p>町田市情報セキュリティポリシーにより規定・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <p>デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p>	<p>町田市情報セキュリティポリシーにより規定・情報セキュリティ対策の遵守状況を検証するため、定期的に情報セキュリティ監査を行っている。監査は情報セキュリティ内部監査と情報セキュリティ外部監査を必要性に応じ、組み合わせて実施している。</p> <p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <p>厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。</p> <p><ガバメントクラウドにおける措置></p> <p>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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う

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6年7月1日	IV その他のリスク対策 ※ 2. 従業員に対する教育・啓発 従業員に対する教育・啓発 具体的な方法	<ul style="list-style-type: none"> ・派遣労働者に対して、セキュリティポリシーの理解と遵守及び情報システムの適正な運用を行うことを目的とする教育を行う。 町田市情報セキュリティポリシーにより規定 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 <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料を作成し、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。	<ul style="list-style-type: none"> ・派遣労働者に対して、セキュリティポリシーの理解と遵守及び情報システムの適正な運用を行うことを目的とする教育を行う。 町田市情報セキュリティポリシーにより規定 ・新規採用職員に対する、セキュリティポリシーの理解と遵守を確実にすることを目的とした教育をしている。 ・すべての職員に対する、情報セキュリティ対策の重要性及び意識向上を目的とした教育をしている。 ・情報システム利用者に対して情報システムの適正な運用を行うことを目的とした教育をしている。 ・情報セキュリティ内部監査員を養成するための教育をしている。 <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料を作成し、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。	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
令和6年7月1日	IV その他のリスク対策 3. その他のリスク対策	<p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <p>デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。</p>	<p><中間サーバー・プラットフォームにおける措置></p> <p>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。</p> <p><新型コロナウイルス感染症対策に係る予防接種事務における追加措置></p> <p>厚生労働省から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。</p>	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
			<p><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。</p>	事前	重要な変更該当する項目の変更が含まれるため、事前に提出・公表を行う
令和6年7月1日	<p>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 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</p>	<p>・端末については、盗難防止具(鍵付チェーン等)を使用している。</p>	<p>・端末については、盗難防止具(鍵付チェーン等)の使用または鍵付キャビネットへの保管を行っている。</p>	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
令和6年7月1日	V 開示請求、問合せ 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	郵便番号194-8520 東京都町田市森野2-2-22 担当課:保健所保健予防課保健予防係、保健 予防課臨時接種推進室 電話:042-725-5422(保健予防課保健予防 係)、042-785-4199(保健予防課臨時接種推進 室) FAX:050-3161-8634	郵便番号194-8520 東京都町田市森野2-2-22 担当課:保健所保健予防課保健予防係 電話:042-725-5422(保健予防課保健予防係) FAX:050-3161-8634	事後	
令和6年7月1日	(別添2)ファイル記録項目	別紙「個人情報業務登録票」及び「個人情報コ ンピュータ処理等登録票」のとおり	別紙「個人情報ファイル簿」のとおり	事後	重要な変更該当しない項目 の変更であるため、事前の提 出・公表が義務付けられない
令和6年7月1日	表紙 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	町田市個人情報保護条例 第1条 この条例は、市民が自己に関する個人 情報の主体であることにかんがみ、市民の自己 に関する個人情報の開示、訂正、利用の中止 等を求める権利を保障するとともに、個人情報 の適正な取扱いを確保することにより個人情報 を保護し、もって市民の基本的人権の擁護と、 市民の信頼に裏付けられた人間尊重の市政を 実現することを目的とする。	(削除)	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない
令和7年4月1日	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	総務部 市政情報課	総務部 法務課	事後	個人情報保護法施行に伴う、 個人情報保護条例に係る記 述の削除のため、重要な変更 に該当しない

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7年4月1日	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 ④個人情報ファイル簿の公表公表場所	総務部 市政情報課	総務部 法務課	事後	個人情報保護法施行に伴う、個人情報保護条例に係る記述の削除のため、重要な変更には該当しない