

(別添2)変更箇所(2)

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4年7月22日	Ⅲ 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	<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>①特定個人情報を抽出したCSVファイルをワクチン接種記録システム(VRS)へ登録する際には、以下のようになっている。</p> <ul style="list-style-type: none"> ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。管理簿に消去の記録を記載する等、消去履歴を残す。 ②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2つの場面に限定している。 ・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し、使用する。 ・本市からの転出者について、本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。 ③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><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>①特定個人情報を抽出したCSVファイルをワクチン接種記録システム(VRS)へ登録する際には、以下のようになっている。</p> <ul style="list-style-type: none"> ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。管理簿に消去の記録を記載する等、消去履歴を残す。 ②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。 ・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する場合のみ入手し、使用する。 ・本市からの転出者について、本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。 ③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。 	事後	特定個人情報保護評価に関する規則第9条第2項の規定によるもの
令和4年7月22日	Ⅲ リスク対策 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の内容	特定個人情報の安全管理措置等の必要な措置を講ずること。	<p>個人情報を取扱う契約において、契約書内に個人情報取扱特記事項として次の内容を明記している。</p> <ul style="list-style-type: none"> ・秘密の保持 ・収集の制限 ・適正な管理のために必要な措置を講じる ・目的外利用及び提供の禁止 ・複写又は複製の禁止 ・持ち出しの禁止 ・承諾を得ていない再委託の禁止 ・資料等の返還 ・従事者への周知 ・必要に応じ随時調査を行う ・事故発生等における報告 	事後	リスクを軽減する修正であり、重要な変更には当たらない
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 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担保	再委託していない	<p>十分に行っている</p> <ul style="list-style-type: none"> ・許可のない再委託を禁止する。 ・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の遵守を義務付ける。 	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 その他の措置の内容	<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>本市、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)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 	<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>本市、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	一部事前 特定個人情報保護評価に関する規則第9条第2項の規定によるもの
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 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		システム調達時における業者の選定について、ISMSやプライバシーマークなど、情報セキュリティ又は個人情報保護に関する第三者認証を取得していることを条件としている。	事後	リスクを軽減する修正であり、重要な変更には当たらない
令和4年7月22日	Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続	<p>[○]接続しない(入手)</p> <p>[○]接続しない(提供)</p>	<p>[]接続しない(入手)</p> <p>[]接続しない(提供)</p>	事後	評価の再実施のため

令和4年7月22日	Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続 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><健康管理システムの運用における措置></p> <p>①ユーザーのアクセス権限は、必要最低限の人数、参照範囲としている。</p> <p>②自己のユーザーID、パスワードは適切に管理し、パスワードが他者に知られることのないよう厳重に管理している。</p> <p>③離席時は必ずログアウトし、なりすましによる操作を防止している。</p> <p>④定められたルールを遵守し適切に運用を行っている。</p> <p>⑤情報漏えい防止などを目的とした、人的セキュリティ研修を実施している。</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、情報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制する仕組みになっている。</p>	事後	評価の再実施のため
令和4年7月22日			<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> <p><中間サーバーの運用における措置></p> <p>中間サーバーとの情報連携する事務を行う職員のみ、事務に則した処理権限を付与し、不適切な入手が行われないように対応する。</p>		評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続 リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続 リスク2: 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><健康管理システムの運用における措置></p> <p>健康管理システムでは操作者のログイン時の認証及び操作内容の記録が実施されるため、不正な操作を抑制する仕組みになっている。</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制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>	事後	評価の再実施のため
令和4年7月22日			<p><中間サーバーの運用における措置></p> <p>自治体中間サーバーとの情報連携する事務を行う職員のみ、事務に則した処理権限を付与し、不適切な提供が行われないように対応する。</p>		評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続 リスクへの対策は十分か		十分である	事後	評価の再実施のため

<p>令和4年7月22日</p>	<p>Ⅲ リスク対策 6. 情報提供ネットワークシステムとの接続 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</p>		<p><中間サーバー・ソフトウェアにおける措置> 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自治体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(Virtual Private Network(ヴァーチャルプライベートネットワーク)の頭文字。公衆回線上に仮想的な専用回線を作り、これを利用することで安全性を高める仕組み。データは認証や暗号化で厳重に保護・管理されるため、漏えいや盗聴などの危険性は低い。)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、自治体中間サーバー・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、自治体中間サーバー・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。</p>	<p>事後</p>	<p>評価の再実施のため</p>
<p>令和4年7月22日</p>	<p>Ⅲ リスク対策 7. 特定個人情報の保管・消去その他の措置の内容</p>	<p><ワクチン接種記録システム> 【物理的対策】 ワクチン接種記録システムは、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。 主に以下の物理的対策を講じている。 ・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>	<p><ワクチン接種記録システムにおける措置> 【物理的対策】 ワクチン接種記録システムは、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。 主に以下の物理的対策を講じている。 ・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>	<p>事後</p>	<p>一部事前 特定個人情報保護評価に関する規則第9条第2項の規定によるもの</p>
<p>令和4年7月22日</p>		<p>【技術的対策】 ワクチン接種記録システムは、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該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>	<p>【技術的対策】 ワクチン接種記録システムは、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該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。 (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>		
<p>令和4年7月22日</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。 ・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。</p>		
<p>令和4年7月22日</p>	<p>Ⅲ リスク対策 8. 監査</p>	<p>[]内部監査</p>	<p>[○]内部監査</p>	<p>事後</p>	<p>リスクを軽減する修正であり、重要な変更にと当たらない</p>

令和4年7月22日	Ⅲ リスク対策 9. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	<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> 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。	<浦安市における措置> ・職員等(非常勤職員等を含む)に対して、個人情報保護に関する研修、内部監査、eラーニングにより意識の向上を行っている。 ・新規で構築したシステムのサーバやインターネットに公開しているサーバに対するセキュリティチェックを外部監査にて行う。 <中間サーバー・プラットフォームにおける措置> ・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、セキュリティ研修等を実施することとしている。 ・中間サーバー・プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。 <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> 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。	事後	特定個人情報保護評価に関する規則第9条第2項の規定によるもの
令和4年7月22日	Ⅲ リスク対策 10. その他のリスク対策	<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> 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」に同意の上、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。	<中間サーバー・プラットフォームにおける措置> 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。 <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」に同意の上、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。	事後	特定個人情報保護評価に関する規則第9条第2項の規定によるもの
令和4年7月22日	Ⅲ リスク対策 1. 特定個人情報ファイル名		(2)統合連携DBファイル	事後	評価の再実施のため
令和4年7月22日	Ⅲ 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。) リスクに対する措置の内容		・システムを利用する職員を限定し、個人ごとにID及びパスワードを設定することで、不適切な方法で特定個人情報の入力・更新をすることができない仕組みとなっている。 ・特定の職員のみログインできるシステムにおいて、ログイン履歴を管理をしているため、誰がいつ何の情報を入手したかがわかるようになっている。 ・申請書等は、当事務において必要な情報のみ記載する様式としている。 ・申請等の受付時、窓口において届出内容や身分証明書などの本人確認書類を確認することで、対象者以外の予防接種履歴等の情報入手を防止している。	事後	評価の再実施のため
令和4年7月22日	Ⅲ 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。) リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ 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		<特定個人情報を入力する際の情報漏えいや紛失リスクに対する措置> ・個人情報保護や取扱いについて、年2回のセキュリティeラーニングや内部監査を行い、市のセキュリティポリシーの周知や、ITに関する一般常識、事故対応の方法等、意識を高める活動をしている。 ・各業務で使用する業務システムから出力される、個人情報が記載された紙媒体については、都度シュレッダーにかけるか、施錠保管を行っている。	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 3. 特定個人情報の使用 リスクに対する措置の内容		統合連携DBサーバにおいて、他システムからのアクセスについては、アクセス可能な情報の範囲を必要範囲に限定するよう、アクセス制御を行っている。	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 3. 特定個人情報の使用 リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 3. 特定個人情報の使用 ユーザ認証の管理		行っている ・個人毎にユーザIDを設定し、ユーザID、パスワードによる認証を行っている。	事後	評価の再実施のため

令和4年7月22日	Ⅲ リスク対策 3. 特定個人情報の使用 その他の措置の内容		システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。操作者は個人まで特定でき、記録は永年保存している。また記録は定期的にセキュリティ責任者が検査・分析を行い、不正なアクセスがないことを確認している。	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 3. 特定個人情報の使用 リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ 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		<従業員が事務外で使用するリスクに対する措置 > ・アクセス権限の発効・失効は、毎年度使用者の見直しを行い、権限表の申請書を元に適切に管理を行っている。	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 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		定めている 個人情報を取扱う契約において、契約書内に個人情報取扱特記事項として次の内容を明記している。 ・秘密の保持 ・収集の制限 ・適正な管理のために必要な措置を講じる ・目的外利用及び提供の禁止 ・複製又は複製の禁止 ・持ち出しの禁止 ・承諾を得ていない再委託の禁止 ・資料等の返還 ・従事者への周知 ・必要に応じ随時調査を行う ・事故発生等における報告	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 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担保		再委託していない	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 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		システム調達時における業者の選定について、ISMSやプライバシーマークなど、情報セキュリティ又は個人情報保護に関する第三者認証を取得していることを条件としている。	事後	評価の再実施のため
令和4年7月22日	Ⅲ 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システムを通じた提供を除く。)		[○]提供・移転しない	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 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)	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 ①事故発生時手順の策定・周知		十分に行っている	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 ②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	事後	評価の再実施のため

令和4年7月22日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 その他の措置の内容		<ul style="list-style-type: none"> ・特定個人情報の漏えい・滅失・毀損のリスクを想定した安全管理体制をセキュリティポリシーで謳っている。 ・漏えい・滅失・毀損を想定した情報セキュリティに関する安全管理規程をセキュリティポリシーで謳っている。 ・特定個人情報の漏えい・滅失・毀損を想定した安全管理体制・規程を年2回のセキュリティトレーニングや内部監査にて、職員へ周知を行っている。 ・特定個人情報の漏えい・滅失・毀損を防ぐために、サーバを堅牢なデータセンターへ設置している。データセンターへは事前の申請でのみ入館可能で、建物の入り口で荷物検査があり、サーバ室へは顔認証による入室管理がなされており、強固なセキュリティ管理がなされている。また、庁舎内にあるサーバ室は、入退室管理簿によって管理されており、サーバ室内はカメラによって執務室から常に監視できるようにしている。紙媒体に関しては、不要な場合は都度シュレッダーをかけ、保管する場合は施錠管理を行っている。 ・特定個人情報の漏えい・滅失・毀損を防ぐために、ウイルス対策ソフトの導入と、不正アクセス対策を実施している。職員のパソコンはUSB等の電磁記録媒体が使用できない状態となっており、業務上必要な時は、使用可能な専用パソコンにて、ウイルスソフトにて確認後、使用可能となっている。 ・特定個人情報ファイルの滅失・毀損が発生した場合に復旧できるよう、庁内ネットワークのファイルサーバは1日3回のバックアップを行っている。 	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 リスクへの対策は十分か		十分である	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 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		<ul style="list-style-type: none"> ・特定個人情報の漏えい、滅失、毀損のリスクに対する措置 ・個人情報が記載されている紙媒体については、都度シュレッダーをかけるか、年4回、機密文書を全庁でまとめて溶解処理にて処分を行っている。 	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 8. 監査		<ul style="list-style-type: none"> [○]自己点検 [○]内部監査 	事後	評価の再実施のため
令和4年7月22日	Ⅲ リスク対策 9. 従業者に対する教育・啓発		<ul style="list-style-type: none"> ・十分にしている ・職員等(非常勤職員等を含む)に対して、個人情報保護に関する研修、内部監査、eラーニングにより意識の向上を行っている。 ・新規で構築したシステムのサーバやインターネットに公開しているサーバに対するセキュリティチェックを外部監査にて行う。 	事後	リスクを軽減する修正であり、重要な変更には当たらない
令和4年7月22日	Ⅳ 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	浦安市 健康センター 〒279-0004 千葉県浦安市猫実一丁目2番5号 TEL047-381-9053(直通)	郵便番号279-8501 千葉県浦安市猫実一丁目1番1号 浦安市総務部法務文書課(情報公開室)	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和4年7月22日	Ⅳ 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 ②請求方法	浦安市個人情報保護条例の規定に基づき、開示・訂正・利用停止請求を受け付ける。	情報公開室又は市ホームページからダウンロードできる「個人情報開示請求書」に必要事項を記載し提出する。なお、身分証明書等により本人等の確認を行う。	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和4年7月22日	Ⅳ 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	浦安市 健康センター 〒279-0004 千葉県浦安市猫実一丁目2番5号 TEL047-381-9053(直通)	郵便番号279-0004 千葉県浦安市猫実一丁目2番5号 浦安市健康こども部健康増進課 電話番号 047-351-1111	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和4年7月22日	Ⅳ 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 ②対応方法	問い合わせの受付時に受付表を作成し、対応について記録を残す。	<ul style="list-style-type: none"> ・問い合わせ等については、電話や窓口にて受付を行い、必要に応じて記録を残す。 ・情報漏えい等に関する問い合わせがあった場合は、必要な対応を行い総務部法務文書課へ報告する。 	事後	その他の項目の変更であり事前の提出・公表が義務付けられない
令和4年7月22日	Ⅴ 評価実施手続 1. 基礎項目評価 ②実施日	令和3年4月1日	令和4年6月30日	事後	評価の再実施のため
令和5年11月22日	Ⅴ 評価実施手続 1. 基礎項目評価 ①実施日	令和4年6月30日	令和5年10月20日	事後	評価再実施に伴う変更