変更点リスク評価表（住民基本台帳）

評価書の変更箇所				変更経緯およびリスク評価			
通番		変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
1	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 （別添１）事務の内容シート	住基ネットGWシステム システム共通基盤（富士通）	住基ネットGWシステムは削除 システム共通基盤はオブジェクトストレージに変更	標準化対応のため既存住基システムパッケージが変更となった。その影響で、住基ネットGWシステムと同じ機能が既存住基システムに盛り込まれ、住基ネットGWシステムは廃止となった。 システム間のデータ連携機能については、システム共通基盤の利用をやめて、ガバメントクラウド上のオブジェクトストレージ経由でデータ連携するよう変更となる。	あり	住基ネットGWシステムは既存住基システムの副本サーバであり、CSと既存住基システムの連携時にデータ変換している。住記データを管理するサーバが減るので、リスクが減るといえる。 データ連携はガバメントクラウド上のオブジェクトストレージ経由で行うよう変更するため、適切なリスク管理が必要となる。	オブジェクトストレージはガバメントクラウド上に構築する。ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。
11	Ⅰ基本情報 ６．情報提供ネットワークによる情報連携 ②法令上の根拠	・番号法第１９条第８号（特定個人情報の提供の制限）及び別表第二 （別表第二における情報提供の根拠） ：第三欄（情報提供者）が「市町村長」の項のうち、第四欄（特定個人情報）に「住民票関係情報」が含まれる項（１、２、３、４、６、８、９、１１、１６、１８、２０、２３、２７、３０、３１、３４、３５、３７、３８、３９、４０、４２、４８、５３、５４、５７、５８、５９、６１、６２、６６、６７、７０、７４、７７、８０、８４、８５の２、８９、９１、９２、９４、９６、９７、１０１、１０２、１０３、１０５、１０６、１０８、１１１、１１２、１１３、１１４、１１６、１１７、１２０の項） （別表第二における情報照会の根拠） ：なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	・番号法第１９条第８号（特定個人情報の提供の制限） ・行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく利用特定個人情報の提供に関する命令（令和6年デジタル庁、総務省令第９号。以下「番号法第１９条第８号に基づく主務省令」という。） （番号法第１９条第８号に基づく主務省令第２条の表における情報提供の根拠） 第三欄（情報提供者）が「市町村長」の項のうち、第四欄（特定個人情報）に「住民票関係情報」が含まれる項（１、２、３、５、７、１１、１３、１５、２０、２８、３７、３９、４８、５３、５７、５８、５９、６３、６５、６６、６９、７３、７５、７６、８１、８３、８４、８６、８７、９１、９２、９６、１０６、１０８、１１０、１１２、１１５、１１８、１２４、１２９、１３０、１３２、１３６、１３７、１３８、１４１、１４２、１４４、１４９、１５０、１５１、１５２、１５５、１５６、１５８、１６０、１６３、１６４、１６５、１６６） （番号法別表における情報照会の根拠）なし （住民基本台帳に関する事務において情報提供ネットワークシステムによる情報照会は行わない）	番号法など一部改正法の施行により、番号法別表第一・別表第二の記載が変更になった。そのため、評価書の記載を修正した。	なし	番号法改正対応で評価書の記載のみ修正し、運用に変更ははいっていない。リスク変化なし。	
14	Ⅱ特定個人情報ファイルの概要 （１）住民基本台帳ファイル ３．特定個人情報の入手・使用 ①入手元		行政機関・独立行政法人等（地方公共団体情報システム機構）	記載漏れがあったため追記した。J-LISよりマイナンバーカード関連情報を受け取っている。	なし	マイナンバーカード交付業務のことを指している。元々運用している業務のため、実際はリスク変化なし。	
89	Ⅱ特定個人情報ファイルの概要 （１）住民基本台帳ファイル ６．特定個人情報の保管・消去 ①保管場所		＜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。	ガバメントクラウドを利用するため、デジタル庁の評価書記載例を転記した。	あり	現行の住民基本台帳ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	ガバメントクラウドでは以下のようなリスク対策をとっている。 ①ISMAPに登録されたクラウド事業者は政府基準に基づいたセキュリティ管理策を実施しており、信頼性が高い。 ②ISO/IEC 27017と27018の認証にて、クラウドサービスのセキュリティ管理と個人情報保護に関する国際基準を満たしている。 ③現行のファイル保管場所と比較したところ、国内のデータセンター保管という運用に変更なし。 ④現行のバックアップ保存場所は本番環境と同じデータセンターだが、今回の変更では本番環境と別のデータセンターに保存されるため、災害時やインシデント発生時に役立つ。
95	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 （１）　住民基本台帳ファイル ２．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）。 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	・既存住基システムには特定個人情報ファイルが保存されない仕組みである。	・既存住基システム用端末には特定個人情報ファイルが保存されない仕組みである	記載内容に誤りがあったため修正した。既存住基システムにつなぐ端末のローカルドライブには特定個人情報ファイルが保存されないため、仮に端末を紛失しても特定個人情報は流出しない。	なし	元々既存住基システムで特定個人情報を管理し、既存住基システムを操作する端末のローカルドライブに特定個人情報が残らない運用をしている。リスク変化なし。	

変更点リスク評価表（住民基本台帳）

評価書の変更箇所				変更経緯およびリスク評価			
通番		変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
96	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 （１） 住民基本台帳ファイル 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	・端末ごとにIDカードとパスワードによる認証を行った後に、端末からシステムを利用する際には、ユーザIDとパスワードによる認証を行っている。	・端末ごとに二要素認証を行った後に、端末からシステムを利用する際には、ユーザIDとパスワードによる認証を行っている。	端末の認証方式に一部変更が入ったため修正した。一部のグループはIDカードではなく生体情報を利用しているため、二要素認証という記載に変更した。	あり	生体情報は個人固有の情報で紛失・盗難が困難なことから、IDカードよりもセキュリティが高い。	
97	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 （１） 住民基本台帳ファイル 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 特定個人情報の使用の記録 具体的な管理方法	・端末から参照、更新した場合のアクセスログを記録している。 ・記録項目：処理日時、職員情報、部署情報、端末情報、処理事由、宛名番号、４情報。	・端末から参照、更新した場合のアクセスログ及び操作ログを記録している。 ・記録項目：処理日時、職員情報、部署情報、端末情報、処理事由、宛名番号、４情報。 ・アクセスログ、操作ログの記録を行い、操作者を特定できるようにする ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する	現在取り組んでいるリスク対策を見直し、操作ログの記録・チェックを追記した。	あり	操作ログの記録・確認することで、不正アクセスの早期発見や内部の不正行為防止に役立てることができる。	
98	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 （１） 住民基本台帳ファイル 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 ⑤物理的対策 具体的な対策の内容	＜データセンター＞ ・外部侵入防止 外周赤外線センサー監視、24時間有人監視、監視カメラ ・入退管理 ICカード+手のひら静脈認証による入退管理、要員所在管理システム ・不正持込・持出防止　金属探知機、生体認証ラック開閉管理、DRタグによる媒体管理	削除	標準化対応のため既存住基システム設置場所をデータセンターからガバメントクラウドへ変更することになった。	あり	現行の住民基本台帳ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	項番99ガバメントクラウドと比較した。 物理的な侵入防止策（入退室管理等）は、データセンターもガバメントクラウドも同程度のセキュリティ対策を実施している。 さらに、ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。
99	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 （１） 住民基本台帳ファイル 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 ⑤物理的対策 具体的な対策の内容		＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。	ガバメントクラウドを利用するため、デジタル庁の評価書記載例を転記した。	あり	現行の住民基本台帳ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	項番98データセンターと比較した。 物理的な侵入防止策（入退室管理等）は、データセンターもガバメントクラウドも同程度のセキュリティ対策を実施している。 さらに、ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。
100	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 （１） 住民基本台帳ファイル 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 ⑥技術的対策 具体的な対策の内容		＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	ガバメントクラウドを利用するため、デジタル庁の評価書記載例を転記した。	あり	現行の住民基本台帳ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。具体的には以下のような技術的対策を実施する。 ①データアクセスを制限する契約 ②モニタリング・ログ管理 ③セキュリティ対策 ④ウイルス対策 ⑤セキュリティパッチ適用 ⑥⑦閉域ネットワーク ⑧データアクセスの技術的制限
101	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 （１） 住民基本台帳ファイル ７．特定個人情報の保管・消去 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 手順の内容		・ガバメントクラウドにおいては、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。	ガバメントクラウドを利用するため、デジタル庁の評価書記載例を転記した。	あり	データ消去プロセスを標準化された手順で行うことで、データ漏えいのリスクが低減される。NIST 800-88は、データの確実な消去を保証するためのガイドラインを提供しており、データが完全に復元不可能になる。	

変更点リスク評価表（住民基本台帳）

評価書の変更箇所				変更経緯およびリスク評価			
通番		変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
102	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） 本人確認情報ファイル 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 ⑥技術的対策 具体的な対策の内容	・不正アクセス対策 ：本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォール（ほかに侵入検知システム（ＩＤＳ）／侵入防御システム（ＩＰＳ）の導入を予定している場合は追記する。）を導入する。	・不正アクセス対策 ：本人確認情報の管理について定めた規程に基づき、ネットワーク管理に係る手順等を整備し、ファイアウォールを導入する。	誤記があったため修正した。住基ネットCSの専用回線で、閉域網のためIDS・IPSは導入していない。	なし	実態は閉域網で元々IDS・IPSは利用しておらず、リスク変化なし。	
103	Ⅳその他のリスク対策 １．監査 ②監査 具体的な内容		・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。	ガバメントクラウドを利用するため、デジタル庁の評価書記載例を転記した。	あり	現行の住民基本台帳ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	ISMAP監査機関により、クラウド事業者が規制やガイドラインに準拠していることが確認される。
104	Ⅳその他のリスク対策 １．監査 ②監査 具体的な内容		・中間サーバー・プラットフォームにおける措置 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。	記載漏れがあったため追記した。中間サーバー・プラットフォームを利用する全自治体が記載することになっている。	なし	中間サーバー・プラットフォームにおける措置は、平成28年頃の中間サーバ導入時よりこの運用をしており、中間サーバー・プラットフォームのリスク対策は地方公共団体情報システム機構が行うため、リスク変化なし。	
105	Ⅳその他のリスク対策 ３．その他のリスク対策		＜中間サーバー・プラットフォームにおける措置＞ 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。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。	中間サーバー・プラットフォームにおける措置は、総務省より示された中間サーバ導入時の評価書修正案を記載した。記載漏れのため今回追記した。 ガバメントクラウドにおける措置は、デジタル庁の評価書記載例を転記した。	あり	中間サーバー・プラットフォームにおける措置は、平成28年頃の中間サーバ導入時よりこの運用をしており、中間サーバー・プラットフォームのリスク対策は地方公共団体情報システム機構が行うため、リスク変化なし。 ガバメントクラウドにおける措置については、今までは豊島区とシステム保守事業者の2者で責任を分担したが、ガバメントクラウド利用によりクラウド事業者にも責任が発生することとなる。	デジタル庁が示す責任分担の考えに則り、適切な判断を行う。ガバメントクラウド起因の事象はクラウド事業者の責任とし、業務アプリケーション起因の事象はシステム保守業者の責任とする。その他については個別具体的に判断していく。
106	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 （別添１）事務の内容シート	証明書自動交付システム（富士通） CSサーバ（富士通） 番号連携SV（富士通）	（富士通）という表記を削除し以下のように変更 証明書自動交付システム CSサーバ 番号連携SV	評価書から事業者名を削除する方針へ変更となった。	なし	事業者名の記載を削除した。該当システムの保有者は自治体であり、事業者はあくまでもシステム保守のみ。図の意図として該当システムの保有者を示すと考えたため修正した。そのためリスク変化なし。	

変更点リスク評価表（個人住民税）

評価書の変更箇所				変更経緯およびリスク評価			
通番	項目	変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
4	Ⅰ基本情報　５．個人番号の利用　法令上の根拠	・番号法第九条及び別表二十四の項 ・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の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号。以下「別表事務省令」という。）第十六条	・番号法第九条及び別表二十四の項 ・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の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号。以下「別表事務省令」という。）第十六条 ・公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律	住民税還付事務において、還付対象者が公金受取口座の利用を申し出ると口座情報の記入が不要となり、情報連携により口座情報を取得し還付口座とする機能を実装するため根拠法令を追記した。	あり	情報連携の機会が増加する。実装必須機能であるため適切なリスク管理を行ったうえで取り扱う必要がある。	情報連携を行うのは還付対象者のうち希望者のみ。 複数の職員で対象者確認を行ったうえで連携し適切な連携を行う。
5	(別添１)事務内容		・オブジェクトストレージ(S3)を追加 ・備考①、④、⑥、⑦、⑮、㉑を追加・修正	システム共通基盤の機能のうち、システム間のデータ連携機能についてはガバメントクラウド上のオブジェクトストレージに移行し、番号連携サーバーの機能のみ残存することから呼称のみを変更するもの	なし	現行のシステム同様の連携となるため、リスク変化を伴わない	
6	Ⅱ　特定個人情報ファイルの概要　２．基本情報　主な記録項目　※		その他(公金受取口座登録・連携ファイル関係情報)	通番4、5と同様			
8	Ⅱ　特定個人情報ファイルの概要　１．特定個人情報ファイル名　（１）個人住民税ファイル　３．特定個人情報の入手・使用　①入手元	行政機関・独立行政法人等(国税庁、日本年金機構)	行政機関・独立行政法人等(国税庁、日本年金機構、デジタル庁)	通番4に伴いデジタル庁を追記したもの。	あり	情報連携の機会が増加する。実装必須機能であるため適切なリスク管理を行ったうえで取り扱う必要がある。	情報連携を行うのは還付対象者のうち希望者のみ。 複数の職員で対象者確認を行ったうえで連携し適切な連携を行う。
12	Ⅱ　特定個人情報ファイルの概要　１．特定個人情報ファイル名　（１）個人住民税ファイル　４．特定個人情報ファイルの取扱いの委託　委託事項１　⑦再委託	再委託しない	再委託する	標準化対応のため全国的なSE不足が発生しているため、標準化対応のシステムの外注を行う必要があるため、修正をしたもの。	あり	再委託を行うことにより特定個人情報に触れる可能性のある者が増える。	・再委託が必要な場合には、あらかじめ委託先から、再委託するものの名称、再委託の内容、再委託先において個人情報を取り扱う責任者及び担当者の氏名等の通知を受け、当該再委託先に関する審査を行い、承認を行っている。 ・再委託を行う場合には、委託先と同様の機密保持規約の遵守を義務づけている。
14	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 個人住民税ファイル　６．特定個人情報の保管・消去　①保管場所　※	＜豊島区における措置＞ ・システム内電子データ ①セキュリティゲートにて生体認証により入退館管理をしている建物の中で、さらに生体認証により入退室管理を行っている部屋に設置したサーバー内に保管する。 ②サーバーへのアクセスについては、二要素認証が必要な端末からのみアクセスすることが可能となる。 ・紙媒体等 事務室内の施錠可能な物品庫、庁舎内の施錠可能な倉庫及び庁舎外の施錠可能な倉庫内に保管する。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜豊島区における措置＞ ・システム内電子データ ①セキュリティゲートにて生体認証により入退館管理をしている建物の中で、さらに生体認証により入退室管理を行っている部屋に設置したサーバー内に保管する。 ②サーバーへのアクセスについては、二要素認証が必要な端末からのみアクセスすることが可能となる。 ・紙媒体等 事務室内の施錠可能な物品庫、庁舎内の施錠可能な倉庫及び庁舎外の施錠可能な倉庫内に保管する。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	ガバメントクラウドを利用するため、デジタル庁の評価書記載を転記した。	あり	現行の個人住民税ファイル保存先からリスク対策が追加されるため、セキュリティリスクは低減する。	ガバメントクラウドでは以下のようなリスク対策をとっている。 ①ISMAPに登録されたクラウド事業者は政府基準に基づいたセキュリティ管理策を実施しており、信頼性が高い。 ②ISO/IEC 27017と27018の認証にて、クラウドサービスのセキュリティ管理と個人情報保護に関する国際基準を満たしている。 ③現行のファイル保管場所と比較したところ、国内のデータセンター保管という運用に変更なし。 ④現行のバックアップ保存場所は本番環境と同じデータセンターだが、今回の変更では本番環境と別のデータセンターに保存されるため、災害時やインシデント発生時に役立つ。

変更点リスク評価表（個人住民税）

評価書の変更箇所				変更経緯およびリスク評価			
通番	項目	変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
20	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 滞納管理ファイル　６．特定個人情報の保管・消去　①保管場所　※	＜豊島区における措置＞ 事務室内の施錠可能な書庫及び庁舎内の施錠可能な倉庫内に保管する。	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜豊島区における措置＞ 事務室内の施錠可能な書庫及び庁舎内の施錠可能な倉庫内に保管する。	通番14と同様			
23	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　１．特定個人情報ファイル名（１）個人住民税ファイル　２．特定個人情報の入手　リスク4：　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	④システム共通基盤（団体内統合宛名システム）からの入手においては、データセンタ内のサーバ間通信に限定されている。	④番号連携サーバー（団体内統合宛名システム）からの入手においては、データセンタ内のサーバ間通信に限定されている。	通番5と同様			
24	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　１．特定個人情報ファイル名（１）個人住民税ファイル　３．特定個人情報の使用　リスク1：目的を超えた紐づけ、事務に必要のない情報との紐づ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	・番号連携サーバー（団体内統合宛名システム）は、個人番号利用業務以外又は個人番号利用業務のうち個人番号を使用しない業務からの要求があった場合には、個人番号を含まない情報のみが提供されるようにアクセス制御されている。 ・番号連携サーバー（団体内統合宛名システム）へは、権限のない者の接続を認めない。	・個人番号利用業務以外又は個人番号利用業務のうち個人番号を使用しない業務からの要求があった場合には、個人番号を含まない情報のみが提供されるようにアクセス制御されている。または権限のない者の接続を認めない。	通番5と同様			
25	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　１．特定個人情報ファイル名（１）個人住民税ファイル　６．情報提供ネットワークシステムとの接続　リスク7：誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク　情報提供ネットワークシステムとの接続に伴うその他リスク及びそのリスクに対する措置	◎情報提供ネットワークシステムとの接続は、すべてシステム共通基盤（団体内統合宛名システム）を介して行われる。	◎情報提供ネットワークシステムとの接続は、すべて番号連携サーバー（団体内統合宛名システム）を介して行われる。	通番5と同様			
26	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　１．特定個人情報ファイル名（１）個人住民税ファイル　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　⑤物理的対策　具体的な対策の内容	＜豊島区における措置＞ ①外部侵入防止措置 外周赤外線センサー監視、２４時間有人監視、監視カメラによる監視。 ②入退室管理 ＩＣカード及び手のひら静脈認証による入退室管理、要員所在管理システムによる管理。 ③不正持込・持出防止措置 金属探知機検査措置、生体認証ラック開閉管理、ＤＲタグによる媒体管理。 ＜中間サーバ・プラットフォームにおける措置＞ 中間サーバ・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。	＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ＜豊島区における措置＞ ①外部侵入防止措置 外周赤外線センサー監視、２４時間有人監視、監視カメラによる監視。 ②入退室管理 ＩＣカード及び手のひら静脈認証による入退室管理、要員所在管理システムによる管理。 ③不正持込・持出防止措置 金属探知機検査措置、生体認証ラック開閉管理、ＤＲタグによる媒体管理。 ＜中間サーバ・プラットフォームにおける措置＞ 中間サーバ・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。	通番14と同様			
27	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　１．特定個人情報ファイル名（１）個人住民税ファイル　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　⑥技術的対策　具体的な対策の内容	＜豊島区における措置＞ ①コンピュータウイルス対策ソフトウェアを導入している。 ②作業端末の仮想化を行っている。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・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・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているＯＳ及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	通番14と同様			

変更点リスク評価表（個人住民税）

評価書の変更箇所				変更経緯およびリスク評価			
通番	項目	変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
			＜豊島区における措置＞ ①コンピュータウィルス対策ソフトウェアを導入している。 ②作業端末の仮想化を行っている。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ・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・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。				
28	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　１．特定個人情報ファイル名（１）　個人住民税ファイル　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　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	＜豊島区における措置＞ 紙等の媒体で提出又は出力された課税情報（特定個人情報）は、保存期間を経過した後、文書管理担当課にて溶解処理する。	＜ガバメントクラウドにおける措置＞ データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ＜豊島区における措置＞ 紙等の媒体で提出又は出力された課税情報（特定個人情報）は、保存期間を経過した後、文書管理担当課にて溶解処理する。	ガバメントクラウドを利用するため、デジタル庁の評価書記載を転記した。	あり	データ消去プロセスを標準化された手順で行うことで、データ漏えいのリスクが低減される。NIST 800-88は、データの確実な消去を保証するためのガイドラインを提供しており、データが完全に復元不可能になる。	
29	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　１．特定個人情報ファイル名（１）　滞納管理システムファイル　３．特定個人情報の使用　宛名システム等における措置の内容	・滞納整理システムとシステム共通基盤（団体内統合宛名システム）との間では、直接の連携はおこなわない。 （参考） システム共通基盤（団体内統合宛名システム）としては、 ①個人番号利用業務以外又は個人番号利用業務のうち個人番号を使用しない業務からの要求があった場合には、個人番号を含まない情報のみが提供されるようにアクセス制御されている。 ②権限のない者の接続を認めない。	・滞納整理システムと番号連携サーバー（団体内統合宛名システム）との間では、直接の連携はおこなわない。	通番5と同様			
30	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　１．特定個人情報ファイル名（２）　滞納管理システムファイル　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 ⑤物理的対策　具体的な対策の内容	＜豊島区における措置＞ ①外部侵入防止措置 外周赤外線センサー監視、２４時間有人監視、監視カメラによる監視。 ②入退室管理 ＩＣカード及び手のひら静脈認証による入退室管理、要員所在管理システムによる管理。 ③不正持込・持出防止措置 金属探知機検査措置、生体認証ラック開閉管理、ＤＲタグによる媒体管理。	＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ＜豊島区における措置＞ ①外部侵入防止措置 外周赤外線センサー監視、２４時間有人監視、監視カメラによる監視。 ②入退室管理 ＩＣカード及び手のひら静脈認証による入退室管理、要員所在管理システムによる管理。 ③不正持込・持出防止措置 金属探知機検査措置、生体認証ラック開閉管理、ＤＲタグによる媒体管理。	ガバメントクラウドを利用するため、デジタル庁の評価書記載を転記した。	あり	保管場所に変更が入るため、セキュリティリスクに変更があると考えられる。	物理的な侵入防止策（入退室管理等）は、データセンターもガバメントクラウドも同程度のセキュリティ対策を実施している。 しかし、ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。
31	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　１．特定個人情報ファイル名（２）滞納管理システムファイル　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　⑥技術的対策　具体的な対策の内容	＜豊島区における措置＞ ①コンピュータウィルス対策ソフトウェアを導入している。 ②作業端末の仮想化を行っている。	＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【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及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ＜豊島区における措置＞ ①コンピュータウィルス対策ソフトウェアを導入している。 ②作業端末の仮想化を行っている。	通番14と同様			

変更点リスク評価表（個人住民税）

評価書の変更箇所				変更経緯およびリスク評価			
通番	項目	変更前	変更後	変更理由	リスク変化	リスク変化の状況	リスク対策
32	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　１．特定個人情報ファイル名（２） 滞納管理システムファイル　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 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	＜豊島区における措置＞ ①滞納整理システムファイルに記録された特定個人情報のデータについては、保管の必要の有無を判別のうえ、バッチ処理にて消去をする。 ②紙等の媒体に出力した滞納整理情報（特定個人情報）は、保存期間を経過した後、文書管理担当課にて溶解処理する。	＜ガバメントクラウドにおける措置＞ データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ＜豊島区における措置＞ ①滞納整理システムファイルに記録された特定個人情報のデータについては、保管の必要の有無を判別のうえ、バッチ処理にて消去をする。 ②紙等の媒体に出力した滞納整理情報（特定個人情報）は、保存期間を経過した後、文書管理担当課にて溶解処理する。	通番28と同様			
33	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　１．特定個人情報ファイル名（３） 扶養等照会ファイル　３．特定個人情報の使用　宛名システム等における措置の内容	・滞納整理システムとシステム共通基盤（団体内統合宛名システム）との間では、直接の連携はおこなわない。 （参考） システム共通基盤（団体内統合宛名システム）としては、 ①個人番号利用業務以外又は個人番号利用業務のうち個人番号を使用しない業務からの要求があった場合には、個人番号を含まない情報のみが提供されるようにアクセス制御されている。 ②権限のない者の接続を認めない。	・扶養等照会ファイルと番号連携サーバー（団体内統合宛名システム）との間では、直接の連携はおこなわない。	通番5と同様			
34	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　１．特定個人情報ファイル名（４） 住民登録地照会ファイル　３．特定個人情報の使用　宛名システム等における措置の内容	・滞納整理システムとシステム共通基盤（団体内統合宛名システム）との間では、直接の連携はおこなわない。 （参考） システム共通基盤（団体内統合宛名システム）としては、 ①個人番号利用業務以外又は個人番号利用業務のうち個人番号を使用しない業務からの要求があった場合には、個人番号を含まない情報のみが提供されるようにアクセス制御されている。 ②権限のない者の接続を認めない。	・住民登録地照会ファイルと番号連携サーバー（団体内統合宛名システム）との間では、直接の連携はおこなわない。	通番5と同様			
35	Ⅳ　その他のリスク対策 ※　１．監査　②監査　具体的な内容	＜豊島区における措置＞ 豊島区情報セキュリティ監査実施計画及び豊島区情報セキュリティ監査実施要綱に基づいて、情報セキュリティ監査を行う。 ＜中間サーバ・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。	＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 ＜豊島区における措置＞ 豊島区情報セキュリティ監査実施計画及び豊島区情報セキュリティ監査実施要綱に基づいて、情報セキュリティ監査を行う。 ＜中間サーバ・プラットフォームにおける措置＞ 運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。	ガバメントクラウドを利用するため、デジタル庁の評価書記載を転記した。	あり	保管場所に変更が入るため、セキュリティリスクに変更があると考えられる。	ガバメントクラウドはISMAPに登録されたクラウド事業者から選定しており、政府が求めるセキュリティ基準を満たしているため、安全性が保障される。 ①データアクセスを制限する契約 ②モニタリング・ログ管理 ③セキュリティ対策 ④ウイルス対策 ⑤セキュリティパッチ適用 ⑥⑦閉域ネットワーク ⑧データアクセスの技術的制限
36	Ⅳ　その他のリスク対策 ※　３．その他のリスク対策	＜中間サーバ・プラットフォームにおける措置＞ 中間サーバ・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。	＜ガバメントクラウドにおける措置＞ ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。 具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。 ＜中間サーバ・プラットフォームにおける措置＞ 中間サーバ・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。	ガバメントクラウドを利用するため、デジタル庁の評価書記載を転記した。	なし	ガバメントクラウドにおける措置については、今までは豊島区とシステム保守事業者の2者で責任を分担したが、ガバメントクラウド利用によりクラウド事業者にも責任が発生することとなる。	デジタル庁が示す責任分担の考えに則り、適切な判断を行う。ガバメントクラウド起因の事象はクラウド事業者の責任とし、業務アプリケーション起因の事象はシステム保守業者の責任とする。その他については個別具体的に判断していく。

個人情報の保護に関する法律施行条例他区事例

〇文京区個人情報の保護に関する法律施行条例

(審議会への諮問等)
第九条　実施機関は、次の各号のいずれかに該当する場合において、個人情報の適正な取扱いを確保するため専門的な知見に基づく意見を聴くことが特に必要であると認めるときは、文京区情報公開制度及び個人情報保護制度運営審議会条例(平成五年三月文京区条例第七号)第一条に規定する文京区情報公開制度及び個人情報保護制度運営審議会(以下「審議会」という。)に諮問することができる。
一　この条例を改正し、又は廃止しようとする場合
二　法第六十六条第一項の規定により講ずる措置の基準を定めようとする場合
三　実施機関における個人情報の取扱いに関する運用上の細則を定めようとする場合

2　実施機関は、審議会が前項の規定による諮問に対応するに当たり、個人情報の取扱いに係る状況を適切に把握するため、毎年一回、当該状況について審議会へ報告するものとする。ただし、実施機関が必要があると認めるときは、随時審議会へ報告することができる。

〇目黒区個人情報の保護に関する法律施行条例

(実施状況の報告及び公表)
第 14 条　区長は、毎年 1 回、実施機関における保有個人情報の取扱いに関する事務の実施状況について取りまとめ、審議会に報告するとともに、公表するものとする。