第三者点検部会の意見内容及び意見を踏まえた修正内容（全項目評価書）

評価書の項目	当初の記載	第三者点検部会時の修正案	第三者点検部会でのご意見	ご意見を受けた修正内容
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	＜データセンターにおける措置＞ 1　外部侵入防止：オペレータによる24時間365日の常駐監視、監視カメラ 2　防犯対策・入退館管理：ICカード認証及び認証ログ管理、12種類アクセスレベル設定、エリア単位の入退室者及び日時等管理、顔認証及び認証ログ管理 3　持込・持出防止：不要又は事前申請のない電子機器等の金属探知機による持ち込み確認、ラックのシリンダ錠による個別施錠、社外持出時セキュリティ管理責任者承認、個人所有のノートPC等の業務使用禁止	現在活用しているデータセンター内でのセキュリティ対策の記載となる。今後は、ガバメントクラウドを利用することになるため、記載を削除。	現在利用しているデータセンターのセキュリティ対策の記載を削除するだけでは、セキュリティが低下したように読み取れる。ガバメントクラウドで実施されているセキュリティ対策を確認し、代わりに記載することが適当。	＜ガバメントクラウドにおける措置①＞ 1　外部侵入防止：監視カメラの設置及び侵入検知システムを導入し、異常検出時に24時間365日対処可能な体制を整えている。 2　防犯対策・入退館管理：データセンターへの入室には二要素認証を導入し、入室の記録を監査している。また、入室の目的等に応じた入室可能範囲が設定されている。 3　持込・持出防止：モバイル機器の使用は管理されている。また、許可のない装置等の持出を禁止している。
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 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	・契約で委託業務実施場所を区が管理する施設に限定し、外部への持出しを禁止している。	リモート保守の対応が可能となることから、委託業務実施場所が区が管理する施設に限定されなくなる。このため、記載を削除。	区のサーバ室等での作業の際に実施していた制限の内容を削除するだけではなく、リモート保守の際に事業者に実施させる制限の内容を代わりに記載することが適当。	・契約で、委託業務実施場所を、区が指定する場所及び委託事業者が申請し区が承認した委託事業者内の場所に限定している。また、当該指定又は承認した場所以外への業務データの持ち出しを禁止している。
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 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	ガバメントクラウドへの移行に伴うリスク対策に関する記載なし	リモート保守の対応が可能となることから、次のリスク対策の記載を追加する。 ・リモート保守を実施する場合やデータ移行作業をする場合は専用区画で実施することとし、入退室をカメラで監視している。 ・保守等に用いる端末へのログインには多要素認証を用いることとし、許可された者以外の作業を禁止している。 ・業務データを取り扱う端末のインターネットへの接続を禁止し、区が許可した時を除き、データの持ち出しを許可していない。	データの持ち出しに一定の基準を設けることが適当。	・リモート保守を実施する場合やデータ移行作業をする場合は専用区画で実施することとし、入退室の記録を残している。 ・保守等に用いる端末へのログインには多要素認証を用いることとし、許可された者以外の作業を禁止している。 ・業務データを取り扱う端末のインターネットへの接続を禁止している。 ・次のような場合を除き、区はガバメントクラウドから保守事業者の環境へのデータの持ち出しを許可していない。 ①ガバメントクラウドへのサイバー攻撃等により、ガバメントクラウド上からデータを退避する必要が生じた場合 ②ガバメントクラウド上のシステムで障害が発生し、クラウド環境では原因が特定できない場合 ③業務データを保管するために利用しているクラウド事業者を変更する場合 ④このほか、ガバメントクラウドからデータを持ち出すことに緊急または相当の必要性があると区が認める場合 ・保守事業者は、ガバメントクラウドからのデータの持ち出しを行った場合、保守事業者の環境に持ち出したデータを保管する必要がなくなった段階で、速やかに返還又は廃棄し、区に報告することとしている。 ・業務データの保守環境からの持ち出しは許可していない。
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 そのほかの措置の内容	・システム運用を行う専用の室では、「コンピュータ室管理基準」で携帯電話、カメラ等の使用を制限している。	サーバ等の装置はガバメントクラウドを利用するため、区のサーバ室での作業はなくなる。このため、記載を削除。	区のサーバ室等での作業の際に実施していた制限の内容を削除するだけではなく、リモート保守の際に事業者に実施させる制限の内容を代わりに記載することが適当。	・委託事業者の業務実施場所において、携帯電話やカメラ等の通信機器や録画機器の使用を、契約で制限している。
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 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	・データセンターに構築し特定個人情報を記録するサーバについては、サーバ設置エリアへの入退室管理、シリンダ錠によるラック施錠、人感センサ付監視カメラによる監視を行う。データセンターは、カメラ監視及び有人監視を常時実施し、事前申請による入館管理を行う。入退館時は、ICカード認証、顔認証及びログ管理を行う。	現在活用しているデータセンター内でのセキュリティ対策の記載となる。今後は、ガバメントクラウドを利用することになるため、記載を削除。	現在利用しているデータセンターのセキュリティ対策の記載を削除するだけでは、セキュリティが低下したように読み取れる。ガバメントクラウドで実施されているセキュリティ対策を確認し、代わりに記載することが適当。	＜ガバメントクラウドにおける措置①＞ 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クラウド事業者は、その従業員に対して、適正な許可のない装置等の外部への持出は認めていない。また、クラウド事業者は、区のデータにアクセスできない措置を講じている。

※重点項目評価書においても、同一の記載がある箇所において同様の修正を行っています。