資料2

個人情報保護管理運営会議　付議事項

件名	AI-OCR の導入に係る外部結合について

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（外部結合）

（担当部課：総合政策部行政管理課、情報システム課）

事業の概要

事業名	AI-OCR の運用
担当課	行政管理課、情報システム課
目　的	紙帳票入力処理時間の短縮及び事務の効率化による業務改善推進のため
対象者	データの入力処理が必要となる申請や報告等を紙帳票で受け付ける者
事業内容	1　概要 乳幼児健診業務で使用する紙帳票の入力処理作業について、AI-OCR を用いた検証を行ったところ、紙帳票の入力処理時間に比べ、約１，５００時間短縮した。 そのため、紙帳票の入力処理の時間短縮や職員の負担軽減を図るため、新たにAI-OCR による事務を導入し、全庁的に展開していく。 2　AI-OCR 利用の流れ （1）紙帳票をスキャナーで読み取り、画像化 （2）LGWAN 回線を介して、AI-OCR へ画像データの取込 （3）画像データから文字データへ自動変換 （4）画像データの確認、変換後の文字データのチェック （5）文字データの編集 （6）文字データのダウンロード 3　システム導入の想定効果 紙帳票の入力処理等と比較し、約３０～４０％の時間短縮 ※個人情報の流れは、資料２－１のとおり

別紙(電子計算機の外部結合関係)

◇外部結合(第３条第1項第３号)

件名　AI-OCR の導入に係る外部結合について

保有課（担当課）	業務主管課（担当課：行政管理課、情報システム課）
登録業務の名称	AI-OCR の運用
結合される情報項目（だれの、どのような項目か）	現時点で想定される帳票の名称等は、資料２－２のとおり
結合の相手方	入札によるため未定 ※LGWAN 回線を利用して接続できるクラウドサービスの提供事業者を予定
結合する理由	クラウドサービスとして提供されている当該システムを有効活用し、各業務主管課で効果的・効率的に運用することで、全庁的な紙帳票の入力処理時間の短縮や文書事務の効率化・業務改善を図るため。
結合の形態	LGWAN 回線を利用して、クラウドサービスとして提供されている当該システムと区のイントラネット端末を接続する。
結合の開始時期と期間	令和５年６月１日（予定）から令和６年３月３１日まで（次年度以降も、同様の外部結合を行う。）
情報保護対策	事業者の情報保護対策 【運用上の対策】 １　個人情報保護法及び事業者策定のプライバシーポリシーや情報セキュリティ方針の遵守 ２　総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」の準拠 ３　ISO/IEC27001:2013,JIS Q 27001/2014（ISMS）認証取得事業者としての情報保護・情報セキュリティ等に係る事項への準拠 【システム上の対策】 １　通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。 ２　ファイアウォールの設置、サーバの要塞化、侵入検知、ウイルス対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。 ３　また、入退室管理・データへのアクセス制限等により、情報資産の危殆化を防止する。 ４　システム・ネットワークの状態、機器操作、サービス利用等について、監視・アクセス等のログを記録する。ログは、必要に応じて分析を行う。

	5　必要に応じて利用者に交付されるID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。 6　システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。 区の情報保護対策 【運用上の対策】 1　個人情報保護法及び情報セキュリティポリシーの遵守 2　区職員への個人情報保護及び情報セキュリティに係る定期な教育 3　必要に応じた区職員による当該クラウドサービス提供事業者への立入調査の実施 4　当該システムの利用状況（所属名・紙帳票の名称・取扱個人情報項目等）の把握・管理 5　必要に応じた個人情報保護審議会への当該システム利用状況の報告 6　紙帳票の施錠保管の実施 7　当該システム上で不要となったデータの削除及び当該システム上で削除した際の削除証明の取得 ※当該システム上にはデータは保管せず、作業終了後、削除する。 【システム上の対策】 1　通信暗号化（SSL/TLS） 2　不正侵入検知・通知･遮断（ファイアウォール/IDS/IPS） 3　Web脆弱性攻撃防止(WAF)・改ざん検知･通報 4　サービス不能攻撃対策(DDoS) 5　標的型攻撃対策による不正通信検知・分析・遮断 6　ふるまい検知・通報・遮断 7　ウイルス対策・セキュリティ更新プログラムの適用 8　通信制御(インターネット分離・特定通信のみ許可) 9　システム監視・通報・バックアップ・脆弱性検査の実施 １０　電子証明書及び多要素認証による利用可能端末の限定 １１　個人単位のユーザ管理・データへのアクセス制御 １２　操作履歴管理、ログ取得 １３　画像データ・文字データへのパスワード付与・暗号化