

個人情報保護管理運営会議 付議事項

件 名	給与明細等のオンライン化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：総務部 人事課）

事業の概要

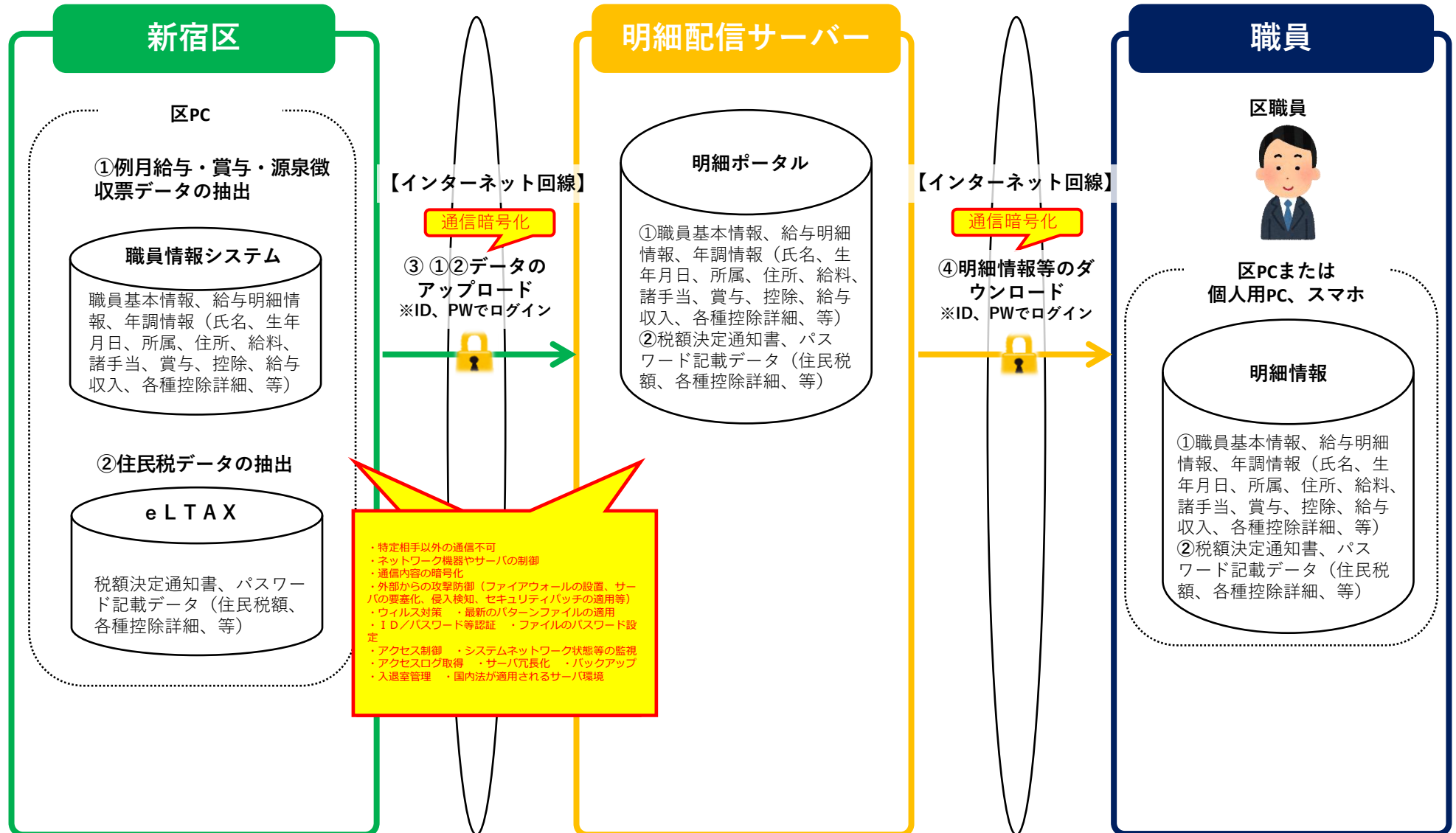
事業名	給与明細等のオンライン化
担当課	総務部人事課
目 的	人事課から職員へ紙で配布する明細類を電子化し、オンライン上にアップロードして各自が閲覧できるようにすることで、ペーパーレス化を推進し、印刷・封入・配送作業の削減による業務改善を目的とする。
対象者	人事課で給与支給する全職員（約 4,200 人）
事業内容	1 概要 人事課から職員へ紙で配布する各種明細については、現在、交換便による配布を行っている。所得税法第 231 条においては、支払を受ける者に対し給与明細書を交付しなければならない旨が規定されており、本人の承諾がある場合には、給与明細書を電子明細にすることができるとしている。また、源泉徴収票についても、所得税法第 226 条において同様の規定が設けられている。 今後は交換便による紙配布を廃止し、システムから出力した各種明細データについて、インターネット回線（通信暗号化）を通じてオンライン明細配信サービスへアップロードする方式に変更する。 これにより、職員は明細ポータルサイト上で、給与・賞与明細、年末調整に係る源泉徴収票、住民税特別徴収税額決定通知書を各自確認できるようにすると共に、ペーパーレス化の推進と、印刷・封入・配送等の事務負担の軽減を図る。 なお、同意がない職員については、各課庶務担当が管理者権限により明細ポータルにアクセスし、該当職員のみ抽出された明細等を印刷して当該職員に紙で配布する。 2 個人情報保護管理運営会議への付議内容 以下について、明細配信サーバーと区のイントラネットの外部結合を行う。 （1）給与または賞与 ⇒ 給与・賞与明細情報（CSV ファイル） （2）所得税源泉徴収票 ⇒ エルタックス送付用給与支払報告書データ（CSV ファイル） （3）住民税決定通知書 ⇒ 住民税通知書ファイル（暗号化 PDF） パスワードファイル（PDF） 3 対象者数 約 4,200 人程度 ※個人情報の流れは、資料 21-1 のとおり

件名 給与明細等オンライン化の外部結合について

保有課(担当課)	人事課
登録業務の名称	① 職員の給与 ② 会計年度任用職員の給与及び費用弁償
結合される情報項目(だれの、どのような項目か)	(対象) 人事課で給与支給対象とする全職員 (項目) 職員基本情報 ・氏名、生年月日、所属、住所等 給与明細情報 ・給料、諸手当、賞与、控除等 年調情報 ・給与収入、各種控除詳細等 住民税情報 ・住民税額、各種控除詳細等
結合の相手方	未定(令和8年8月頃指名競争入札により確定予定)(プライバシーマーク等取得事業者を予定)
結合する理由	人事課で職員に紙で配布する各種明細について、交換便による配布を廃止し、システムから出力したデータをオンライン明細配信サービスへアップロードする方式に変更するため。
結合の形態	区イントラネットパソコンからインターネット回線(通信暗号化)により、明細等情報をアップロードする。
結合の開始時期と期間	令和8年10月から令和9年3月まで(次年度以降も、同様の外部結合を行う。)
情報保護対策	別紙チェックリストのとおり

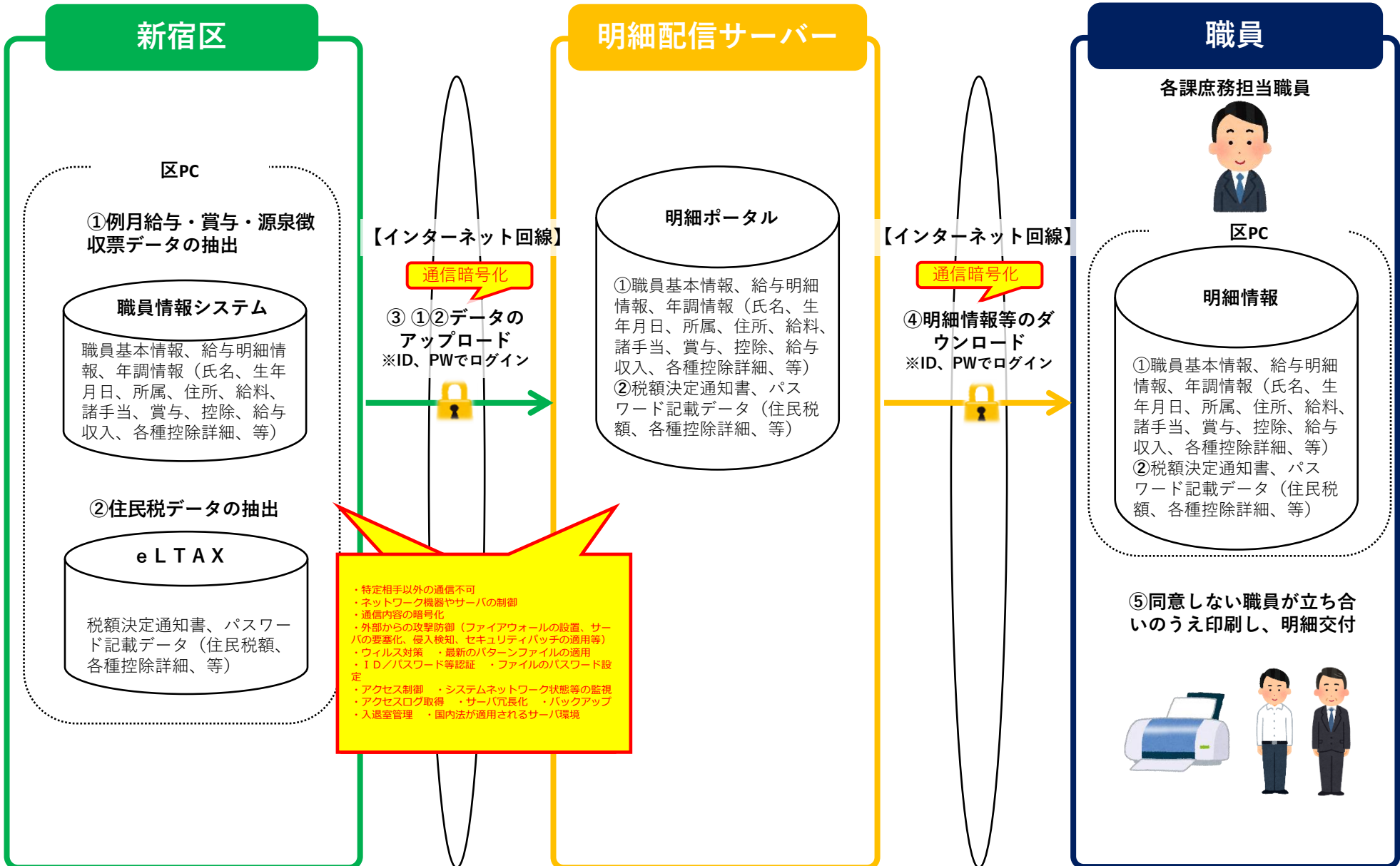
給与明細等のオンライン化に係る外部結合について (同意がある場合)

(資料 2 1 - 1)



給与明細等のオンライン化に係る外部結合について (同意がない場合)

(資料 2 1 - 2)



4 外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
区が行う情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、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」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
区が行う情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	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。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、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。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	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。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	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。

4 外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
結合先に行わせる 情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、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」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
結合先に行わせる 情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、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させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	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、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	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させる。