資料43

個人情報保護管理運営会議　付議事項

件名	区職員の中央労働金庫貯蓄金等のデータ授受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	新宿区職員給与条例控除事務（職員の中央労働金庫貯蓄金等に関する事務）
担当課	総務部人事課
目　的	中央労働金庫の貯蓄金等を利用する職員について、給与からの控除を適切に行うため。
対象者	中央労働金庫の貯蓄金等について給与控除を利用する職員
事業内容	１　概要 中央労働金庫の貯蓄金への積立て並びに貸付金の返還金及び利子について、職員が給与からの控除を申し込んだ場合、人事課では毎月、中央労働金庫から控除依頼データを受領し、当該データに基づき給与控除を行っている。給与控除後は、人事課が控除結果データを作成して中央労働金庫へ送付し、中央労働金庫において貯蓄金の積立て等の処理を行っている。 現在、中央労働金庫とのデータ授受はDVD等の電磁的媒体により行っているが、令和８年12月から、媒体の紛失・誤配送等による情報漏えいリスクの低減及び業務の効率化を図るため、NRIセキュアテクノロジーズ株式会社が提供するクラウド型ファイル交換サービス「クリプト便」を利用し、インターネット回線を介してデータを送受信する方式に変更する。 ２　個人情報保護管理運営会議への付議内容 控除依頼データ及び控除結果データの授受にあたり、NRIセキュアテクノロジーズ株式会社が提供するクラウド型ファイル交換サービス「クリプト便」と外部結合を行う。 ３　対象者数 ２０７名 ※令和８年８月分控除依頼件数 ※個人情報の流れは、資料４３－１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)

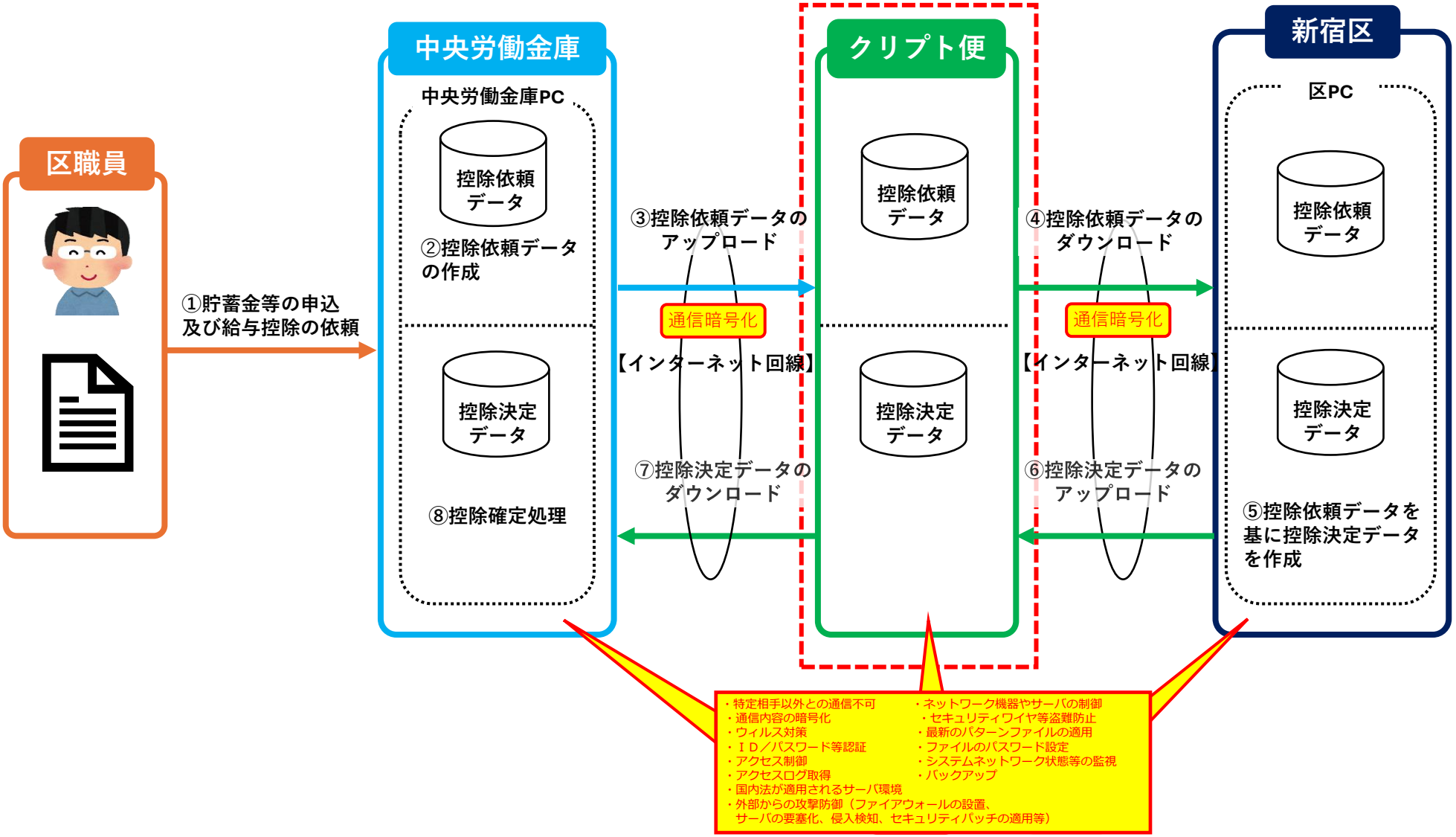
件名　区職員の中央労働金庫貯蓄金等のデータ授受に係る外部結合について

保有課（担当課）	総務部人事課
登録業務の名称	給与条例控除
結合される情報項目（だれの、どのような項目か）	中央労働金庫に対する貯蓄金並びに、これらの法人の貸付金に係る返還金及び利子にかかる次の情報項目 １対象者 中央労働金庫の貯蓄金等について給与控除を利用する職員 ２情報項目 （１）控除依頼データ 控除年月、職場番号、職員番号、氏名、貯蓄金額、返還金額、処理コード （２）控除結果データ 控除月、処理コード、異動コード控除結果コード、職員番号、旧職場番号、新職場番号、氏名、貯蓄金額、返還金額、識別コード
結合の相手方	ＮＲＩセキュアテクノロジーズ株式会社（ＩＳＯ/ＩＥＣ２７００１取得）
結合する理由	現行、媒体により行っているデータ授受について、情報漏えい、媒体・読込機器の継続性、スケジュール遅延等の各リスクを軽減し、業務効率化を図る観点よりインターネットを利用した方法に変更するため。
結合の形態	インターネット回線により、区のイントラネット端末をＮＲＩセキュアテクノロジーズ株式会社が提供する、ファイル交換サービス（クリプト便）と接続する。
結合の開始時期と期間	令和８年１２月１６日から令和９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	別紙チェックリストのとおり

区職員の中央労働金庫との貯蓄金等データ授受に係る個人情報の流れ

（資料４３－１）

※赤字の部分が今回の付議事項



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。