

個人情報保護管理運営会議 付議事項

件名	納税証明の電子連携に係る軽自動車税納付確認システムとの外部結合等について（情報項目の追加等）
----	--

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（電算処理、外部結合）

（担当部課：総務部税務課）

事業の概要

事業名	軽自動車税（種別割）納税確認方法のシステム化
担当課	税務課
目 的	地方税法及び道路運送車両法等に基づき、地方税共同機構が運営する軽自動車税納付確認システム（以下「軽 JNKS」という。）に、区から納付情報を送信し、継続検査時の納税確認を電子的に行うことにより、納税義務者の利便性向上を図る。
対象者	新宿区で課税する小型二輪、三輪及び四輪車の軽自動車税（種別割）納税義務者（法人を含む）
事業内容	1 概要 現在、三輪及び四輪車の軽自動車税について、区はその納付情報を軽 JNKS に LGWAN 回線経由で送信している。税制改正に伴い、令和 7 年 3 月以降は、小型二輪車についても同様の取扱いとし、その軽自動車税の納付状況を軽 JNKS に登録することとする。 これにより、三輪及び四輪車の軽自動車と同様に、小型二輪車についても継続検査（車検）時に納税証明書の提出が不要になる。 また、小型二輪車の軽自動車税の納付状況を軽 JNKS に登録するにあたって、区の保有している軽自動車税情報の精度を向上させるため、道路運送車両法の規定に基づき登録を受けた機関である一般財団法人自動車検査登録情報協会が運営する自動車検査登録情報提供サービス（以下「AIRIS」という。）との外部結合を行う。 2 個人情報保護管理運営会議への付議内容 （1）電算処理 軽 JNKS の対象に小型二輪の納付情報を追加する。 （2）外部結合 ・区イントラネットと軽 JNKS の外部結合の対象車種を変更し、小型二輪を追加する。 ・区イントラネットと AIRIS の外部結合を開始し、区の保有している軽自動車税情報と AIRIS から取得した車検証情報を突合する。 3 想定件数 約 3,200 件（令和 5 年度当初課税件数） ※個人情報の流れは、資料 9－1 のとおり

件名 軽自動車税納付確認システムの導入に伴う税務システムの改修について

※太字ゴシック(下線)が、令和3年度第6回情報公開・個人情報保護審議会からの変更箇所

保有課(担当課)	税務課
登録業務の名称	軽自動車税(種別割)
記録される情報項目(だれの、どのような項目が、どこにコンピュータに記録されるのか)	1 個人の範囲 軽自動車税(種別割)の納税義務者 2 記録項目 資料9-2のとおり 3 記録するコンピュータ 税務システム(委託事業者がパッケージシステムを区の統合基盤上に構築する)
新規開発・追加・変更の理由	軽 JNKS へ送信する軽自動車税(種別割)納付情報において <u>小型二輪車を追加して</u> 作成する機能が必要になるため。
新規開発・追加・変更の内容	既存の税務システムに以下の機能を追加する。 1 税務システム(収納システム)から軽 JNKS への <u>小型二輪車</u> の納付情報連携データの作成 2 税務システム(軽自動車税システム)から <u>小型二輪車</u> の廃車・ナンバー変更等の異動情報を抽出し、軽 JNKS への納付情報の連携データの作成
開発等を委託する場合における個人情報保護対策	<u>別紙チェックリストのとおり</u>
新規開発・追加・変更の時期	令和6年7月(予定) 開発 令和6年10月(予定) テスト 令和7年4月 運用開始

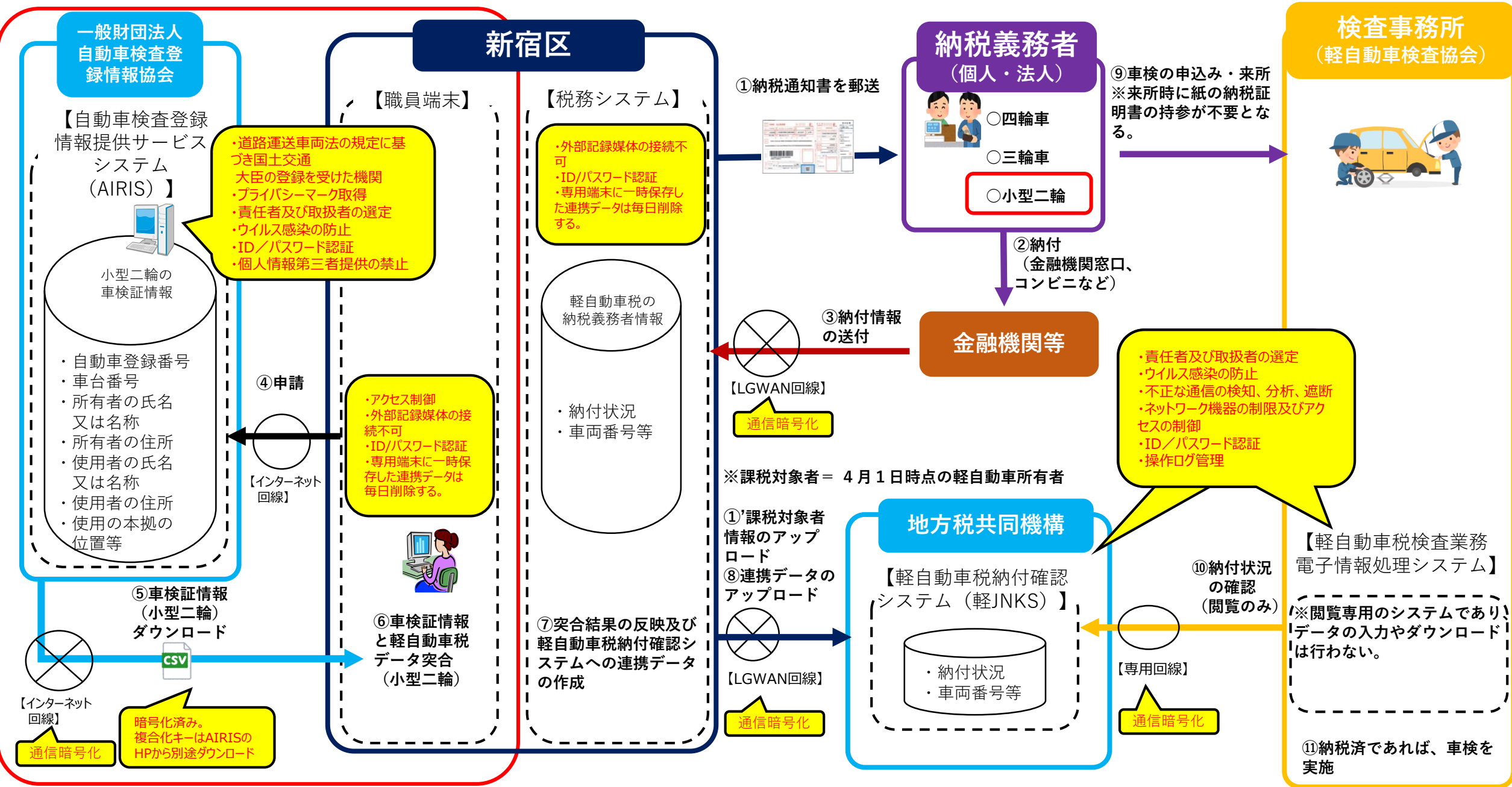
件名 納税証明の電子連携に係る軽自動車税納付確認システムとの外部結合について

※太字ゴシック(下線)が、令和3年度第6回情報公開・個人情報保護審議会からの変更箇所

保有課(担当課)	税務課
登録業務の名称	軽自動車税(種別割)
結合される情報項目(だれの、どのような項目か)	対象者:軽自動車税(種別割)の納税義務者 情報項目:資料9-2のとおり
結合の相手方	地方税共同機構
結合する理由	税法改正に伴い、全国一律で稼働する軽 JNKS において 小型二輪車 の納付情報送信に対応するため
結合の形態	区の LGWAN 端末と軽 JNKS を、LGWAN 回線(地方公共団体を相互に接続する行政専用の総合行政ネットワーク)で結合し、データの送信を行う。
結合の開始時期と期間	令和7年4月1日(次年度以降も、同様の外部結合を行う。) (<u>令和6年10月1日から10月31日まで</u> 仮稼働テスト(個人情報なし)のため、 区の LGWAN 端末と軽 JNKS との外部結合を行う。)
情報保護対策	別紙チェックリストのとおり

件名 納税証明の電子連携に係る自動車検査登録情報提供サービスとの外部結合について

保有課（担当課）	税務課
登録業務の名称	軽自動車税（種別割）
結合される情報項目（だれの、どのような項目か）	対象者：軽自動車税（種別割）の納税義務者 情報項目：資料9－3のとおり
結合の相手方	一般財団法人自動車検査登録情報協会 （道路運送車両法の規定に基づき国土交通大臣の登録を受けた登録情報提供機関、プライバシーマーク取得済）
結合する理由	税法改正に伴い、全国一律で稼働する軽 JNKS への小型二輪納付情報の送信にあたり、事前に区の保有している軽自動車税情報と AIRIS から取得した車検証情報を突合し、情報を精査する必要があるため。
結合の形態	区のイントラ端末と AIRIS とを、暗号化されたインターネット回線で結合し、データの送信を行う。
結合の開始時期と期間	令和6年8月1日（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



※三輪車及び四輪車の車検証情報の突合について別途実施

軽自動車税納付確認システムに係るデータ項目

軽自動車税（種別割）の納付確認業務に係る項目

納税情報登録、車両情報、車両番号（標板番号、分類番号、かな文字、一連番号）、車台番号、全国地方公共団体コード、車種コード、課税年度、納付状況コード、有効年月日、抹消フラグ、更新年月日、改行コード

自動車検査登録情報提供サービスシステムに係るデータ項目**軽自動車税（種別割）の車検証情報に係る項目**

自動車登録番号、車台番号、所有者の氏名又は名称、所有者の住所、使用者の氏名又は名称、使用者の住所、使用の本拠の位置、登録年月日／交付年月日、初度登録年月、総排気量又は定格出力、燃料の種類、型式指定番号、類別区分番号、車名、乗車定員、最大積載量、車両重量、車両総重量、型式、原動機の型式、長さ、幅、高さ、前前軸重、前後軸重、後前軸重、後後軸重、自動車の種別、用途、自家用・事業用の別、車体の形状、有効期限の満了する日、閲覧条件

3 電算処理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
開発等を委託する場合 における区が行う 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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、管理（申請、承認、記録）を行う。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告を求め、区が承認した後に実施するよう指導するとともに、個人情報データの持出しを禁止する。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使うよう指導する。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員が立ち会う。
開発等を委託する場合 における区が行う 情報保護対策 【システム上の対策】	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施し、十分な検証を行う。
	○	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。

3 電算処理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「－」	情報保護対策
開発等を委託する場合 における委託先に行わせる 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。
	○	区のシステム機器設置場所へ委託先が入退室する場合は、区の管理（申請、承認、記録）に従わせる。また、委託先がシステム機器を操作する場合には、事前に作業内容の報告をさせ、区が承認した後に実施させるとともに、個人情報データの持出しを禁止させる。
	○	プログラムの移行等を行う場合は、外部記録媒体の管理を行い、利用時は第三者漏えいがないようパスワードを施す等、利用制限を設ける。
	○	入力及び取込みテストにおいては、ダミーデータを使わせる。
	○	実データを使用した検証作業は、区職員が実施する（委託先には、必要な支援のみ行わせる）。
	○	モバイルパソコン等の電子計算組織を持ち込む場合は、事前に区の許可をとらせ、用途は、社内事務連絡、設計書等の閲覧に限定させる。また、委託先のモバイルパソコン等と区のネットワーク、システム機器及びUSB等の記録媒体と接続をさせないように、区の職員の立会いに応じさせる。
	○	データ項目定義の修正漏れによるシステム不具合等が無いよう、双方で事前に綿密なスケジュール計画やチェックシートを作成して実施する。なお、稼働にあたっては必ず仮移行を行うこととし、本稼働はシステムを使用していない時間帯（時間外・休日）に実施させ、十分な検証を行わせる。
開発等を委託する場合 における委託先に行わせる 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。

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「－」	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。