1　目的外利用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○	情報保護対策
情報保護対策 【運用上の対策】		担当課の保護管理者は、他の行政機関等に保有個人情報を提供するという目的外利用を行うことについて、相当又は特別な理由があると判断できるか、関係部署と慎重に協議する。また、必要に応じて、個人情報保護委員会へ助言を求める。
		担当課の保護管理者は、利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面を取り交わす。
		担当課の保護管理者は、提供先に対し、次に掲げる措置を講ずるよう求める。 ⑴利用目的又は方法の制限 ⑵取扱者の範囲の限定 ⑶第三者への再提供の制限又は禁止 ⑷消去、返却等利用後の取扱いの指定 ⑸取扱状況に関する所要の報告の要求 ⑹訂正の決定を行った場合において、当該訂正に応じる。 ⑺適切な情報保護対策、情報セキュリティ対策の実施
		担当課の保護管理者は、必要があると認めるときは、外部提供を行う前又は随時に実地の調査等を行うことにより、当該措置の状況を確認し、その結果を記録するとともに、改善要求等を行う。
		担当課の保護管理者は、目的外利用により提供する個人情報の取扱者を指定する。

2　外部提供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○	情報保護対策
情報保護対策 【運用上の対策】		担当課の保護管理者は、他の行政機関等に保有個人情報を提供することについて、相当又は特別な理由があると判断できるか、関係部署と慎重に協議する。また、必要に応じて、個人情報保護委員会へ助言を求める。
		担当課の保護管理者は、利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面を取り交わす。
		担当課の保護管理者は、提供先に対し、次に掲げる措置を講ずるよう求める。 ⑴利用目的又は方法の制限 ⑵取扱者の範囲の限定 ⑶第三者への再提供の制限又は禁止 ⑷消去、返却等利用後の取扱いの指定 ⑸取扱状況に関する所要の報告の要求 ⑹訂正の決定を行った場合において、当該訂正に応じる。 ⑺適切な情報保護対策、情報セキュリティ対策の実施
		担当課の保護管理者は、必要があると認めるときは、外部提供を行う前又は随時に実地の調査等を行うことにより、当該措置の状況を確認し、その結果を記録するとともに、改善要求等を行う。
		担当課の保護管理者は、提供する個人情報の取扱者を指定する。

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「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。
		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。
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】		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「ー」	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、十分な検証を行させる。
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「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。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
委託にあたり区が行う情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
		取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
		全体の業務フローを作成し、委託先と共有する。
		個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
		個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
		個人情報は、施錠できる金庫又はキャビネット等に保管する。
		業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に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、委託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、直ちに委託先と今後の対応を協議する。
委託にあたり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。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
委託事業者に行わせる情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
		取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
		区が作成した業務フローに基づき、業務を行わせる。
		個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
		個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
		個人情報は、施錠できる金庫又はキャビネット等に保管させる。
		業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に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。
委託事業者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。

6　業務委託にかかる個人情報保護対策チェックリスト

（紙媒体のみの取扱い）

	・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
委託にあたり区が行う情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
		取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
		全体の業務フローを作成し、委託先と共有する。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
		個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
		個人情報は、施錠できる金庫又はキャビネット等に保管する。
		業務履行後、個人情報が記録された紙媒体は返却するよう指導する。
		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、委託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、直ちに委託先と今後の対応を協議する。

6　業務委託にかかる個人情報保護対策チェックリスト

（紙媒体のみの取扱い）

	・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
委託事業者に行わせる情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
		取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
		区が作成した業務フローに基づき、業務を行わせる。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
		個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
		個人情報は、施錠できる金庫又はキャビネット等に保管させる。
		業務履行後、個人情報が記録された紙媒体は返却させる。
		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。

7　指定管理にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
指定管理にあたり区が行う情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を実施するとともに、指定管理先に対し速やかに状況報告をするよう指導する。
		取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
		全体の業務フローを作成し、指定管理先と共有する。
		個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
		個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
		個人情報は、施錠できる金庫又はキャビネット等に保管する。
		業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に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、指定管理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、直ちに指定管理先と今後の対応を協議する。
指定管理にあたり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。

7　指定管理にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・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
指定管理事業者に行わせる情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、指定管理先に対し速やかに状況報告をさせる。
		取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
		区が作成した業務フローに基づき、業務を行わせる。
		個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
		個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
		個人情報は、施錠できる金庫又はキャビネット等に保管させる。
		業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に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。
指定管理事業者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。

8　指定管理にかかる個人情報保護対策チェックリスト

（紙媒体のみの取扱い）

	・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
指定管理にあたり区が行う情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を実施するとともに、指定管理先に対し速やかに状況報告をするよう指導する。
		取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
		全体の業務フローを作成し、指定管理先と共有する。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
		個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
		個人情報は、施錠できる金庫又はキャビネット等に保管する。
		業務履行後、個人情報が記録された紙媒体は返却するよう指導する。
		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、指定管理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、直ちに委託先と今後の対応を協議する。

8　指定管理にかかる個人情報保護対策チェックリスト

（紙媒体のみの取扱い）

	・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
指定管理事業者に行わせる情報保護対策【運用上の対策】		契約にあたり、「特記事項」を付すとともに、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。
		契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、指定管理先に対し速やかに状況報告をさせる。
		取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
		区が作成した業務フローに基づき、業務を行わせる。
		個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
		個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
		個人情報は、施錠できる金庫又はキャビネット等に保管させる。
		業務履行後、個人情報が記録された紙媒体は返却させる。
		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。