

個人情報保護管理運営会議 付議事項

件 名	図書館情報システムにおけるシステムの更新等について
--------	---------------------------

内容は別紙のとおり

要綱の根拠

◇第3条第1項第3号（電算処理、業務委託）

（担当部課：中央図書館）

事業の概要

事業名	図書館情報システム更新業務委託
担当課	中央図書館
目 的	図書館情報システムの更新によるサービスの向上のため
対象者	図書館情報システムで利用者登録されている個人利用者（区内在住、都内在住、区内在勤、区内在学）
事業内容	1 概要 現在、図書館情報システムにおいては、5年から7年を周期として、プロポーザル方式で選定された事業者がシステム更新を行っている。（平成元年度第15回東京都新宿区個人情報保護審議会で承認済み） この度、システムの更新時期を迎えたため、プロポーザル方式により委託事業者を選定したところ、トーテックアメニティ株式会社が選定された。 今回のシステム更新にあたり、トーテックアメニティ株式会社が導入する図書館情報システム「iLisfiera（アイリスフィエラ）」は、富士通 Japan 株式会社が開発元となっており、新システムへのデータ移行及びシステムのカスタマイズ作業においては、富士通 Japan 株式会社へ再委託を依頼することで、システム更新業務を安全かつ効率的に実施する。 2 個人情報保護管理運営会議への付議内容 （1）電算処理 新たな図書館情報システムへのデータ移行及びシステムのカスタマイズ作業を行う。 （2）業務委託 システムの更新にあたり、機器更新及びシステム更新業務を委託する。 （3）業務委託（再委託） システムの更新にあたり、富士通 Japan 株式会社に現行システムからのデータ移行等を再委託する。 3 対象者数 図書館情報システムに登録された個人利用者 約112,000人 ※個人情報の流れは、資料55－1のとおり

件名 図書館情報システムにおけるシステムの更新について

※太字ゴシック(下線)は、平成元年度第15回東京都新宿区個人情報保護審議会承認済の内容からの変更箇所

保有課(担当課)	中央図書館
登録業務の名称	図書館情報システム
記録される情報項目(だれの、どのような項目が、どこのコンピュータに記録されるのか)	1 個人の範囲 図書館情報システムで利用者登録されている個人利用者 2 記録項目 利用者番号、氏名、生年月日、住所、電話番号、メールアドレス、図書館資料の貸出・予約情報、小学生以下の場合は保護者氏名 3 記録するコンピュータ 次期図書館情報システムサーバ (中央図書館内サーバ室に設置)
新規開発・追加・変更の理由	システム更新によるサービス向上のため、プロポーザル方式により委託事業者を選定し、サーバ機器類及び図書館情報システムの更新を行う。
新規開発・追加・変更の内容	図書館情報システムにおける機器更新及びシステムの更新業務のため。
開発等を委託する場合における個人情報保護対策	別紙チェックリストのとおり
新規開発・追加・変更の時期	令和6年7月 開発 令和6年12月 テスト 令和7年1月 本稼働

件名 図書館情報システムにおけるシステム更新に係る業務の委託について**※太字ゴシック(下線)は、平成元年度第15回東京都新宿区個人情報保護審議会承認済の内容からの変更箇所**

保有課(担当課)	中央図書館
登録業務の名称	図書館情報システム
委託先	トーテックアメニティ株式会社
委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	《図書館情報システムで利用者登録されている個人利用者の情報》 利用者番号、氏名、生年月日、住所、電話番号、メールアドレス、 図書館資料の貸出・予約情報、小学生以下の場合は保護者氏名
処理させる情報項目の記録媒体	電磁的媒体(次期図書館情報システムサーバ) (中央図書館内サーバ室に設置。)
委託理由	<u>上記委託先はプロポーザル方式により選定されたシステム業者であり、システム更新業務を安全かつ効率的に行うことができるため。</u>
委託の内容	<u>図書館情報システムに係る機器更新及びシステム更新業務</u>
委託の開始時期及び期限	<u>令和6年7月10日から令和7年3月31日まで</u> (次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

件名 図書館情報システムにおけるシステム更新に係る業務の再委託について

※太字ゴシック(下線)は、平成元年度第15回東京都新宿区個人情報保護審議会承認済の内容からの変更箇所

保有課(担当課)	中央図書館
登録業務の名称	図書館情報システム
委託先(再委託先)	富士通 Japan 株式会社(プライバシーマーク及びISO27001を取得)
再委託に伴い事業者処理させる情報項目(だれの、どのような項目か)	《図書館情報システムで利用者登録されている個人利用者の情報》 氏名、生年月日、住所、電話番号、メールアドレス、 図書館資料の貸出・予約情報、小学生以下の場合は保護者氏名
処理させる情報項目の記録媒体	電磁的媒体(次期図書館情報システムサーバ) (中央図書館内サーバ室に設置)
再委託理由	<u>富士通 Japan 株式会社は今回導入される図書館情報システム「iLisfiera(アイリスフィエラ)」の開発元であり、委託業者より現行システムからの確実なデータ移行及びシステムのカスタマイズ作業を実現するためには開発元への再委託が必要不可欠である旨の申し出があった。</u> <u>当該再委託については、記録媒体である次期図書館情報システムサーバの設置場所が中央図書館内サーバ室であること、構築環境が中央図書館内であること、委託先のトーテックアメニティ株式会社が共同でシステム構築にあたっていることから、個人情報の取扱いの安全性を十分に確保できると判断できるため、この再委託を承諾する。</u>
再委託の内容	<u>現行システムからのデータ移行作業やカスタマイズ作業</u>
再委託の開始時期及び期限	<u>令和6年7月10日から令和7年3月31日まで</u> (次年度以降も、同様の業務委託を行う。)
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり。
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり。

新宿区
(中央図書館)

- ・電磁的媒体（現行サーバ、次期サーバ）の保管場所・・・中央図書館内サーバ室（持出しなし）
- ・委託先、再委託先が共同でシステム構築を行う場所・・・中央図書館内システム更新業務室
- ・個人情報を含むデータ移行の手段・・・サーバ間通信による。

現行の図書館情報
システムサーバ

利用者情報

利用者番号、氏名、
生年月日、住所、
電話番号、メール
アドレス、貸出・
予約情報、保護者
氏名

- ・データ移行、検証
- ・システムカスタマイズ

委託先
(トーテックアメニティ
株式会社)

再委託先
(富士通Japan株式会社)
(次期システム開発元)

トーテックアメニティ株式会社と
富士通Japan株式会社の作業チーム
が共同でデータ移行等の業務を行う。

次期図書館情報
システムサーバ

利用者情報

利用者番号、氏名、
生年月日、住所、
電話番号、メール
アドレス、貸出・
予約情報、保護者
氏名

現行システム：Lics-Re2(リックスアールイー2)
現行ベンダー：NECネクサソリューションズ株式会社
システム開発元：NECネクサソリューションズ株式会社

- ・特定相手以外との通信不可
- ・ネットワーク機器やサーバの制御
- ・通信内容の暗号化
- ・外部からの攻撃防御（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）
- ・ウィルス対策
- ・最新のパターンファイルの適用
- ・ID/パスワード等認証
- ・ファイルのパスワード設定
- ・アクセス制御
- ・システムネットワーク状態等の監視
- ・アクセスログ取得
- ・サーバ冗長化 ・バックアップ
- ・入退室管理
- ・国内法が適用されるサーバ環境

- ・特記事項等の遵守
- ・立入調査等及び状況報告
- ・責任者及び取扱者の報告
- ・区が作成した業務フローに基づく業務の履行
- ・データの暗号化
- ・事故等への対応体制及び手順の整備
- ・事故発生時等の協議

- ・特定相手以外との通信不可
- ・ネットワーク機器やサーバの制御
- ・通信内容の暗号化
- ・外部からの攻撃防御（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）
- ・ウィルス対策
- ・最新のパターンファイルの適用
- ・ID/パスワード等認証
- ・ファイルのパスワード設定
- ・アクセス制御
- ・システムネットワーク状態等の監視
- ・アクセスログ取得
- ・サーバ冗長化 ・バックアップ
- ・入退室管理
- ・国内法が適用されるサーバ環境

次期システム：iLisfiera(アイリスフィエラ)
次期ベンダー：トーテックアメニティ
システム開発元：富士通Japan株式会社

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。
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】	○	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。
	○	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「－」	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ある場合は、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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
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「－」	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ある場合は、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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
	－ (電子データのみ の取扱いのため)	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。
委託事業者に行わせる 情報保護対策 【システム上の対策】	○	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。
	○	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。