資料58

個人情報保護管理運営会議　付議事項

件名	電子図書サービスの導入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：教育委員会事務局教育支援課）

事業の概要

事業名	学校図書館の充実
担当課	教育支援課
目　的	区立学校への電子図書サービスの導入
対象者	区立学校に在籍する児童・生徒・教員
事業内容	1　概要 現在、区立学校図書館で閲覧できる図書は、紙の図書に限られており、児童・生徒の不読率（本を読まない児童・生徒の割合）の軽減や、授業での探究的な学習等を行う目的とした書籍の活用が求められている。 そのため、令和７年４月より、クラウド型の電子図書サービスを導入することで、児童・生徒及び教員は、１人１台貸与のＧＩＧＡスクールタブレット端末（以下「ＧＩＧＡ端末」という。）を用いた電子図書の閲覧ができるようになり、自宅・教室・職員室などにおいて、読書活動や調べ学習、授業に活用していく。 2　個人情報保護管理運営会議への付議内容 事業者が提供する電子図書サービスと外部結合し、学校（教員）にてインターネットブラウザから当該システムに児童・生徒及び教員の情報を入力し、ユーザーアカウント登録を行う。 3　対象者数 令和７年度：小・中学校　約１，０００人 小学校モデル校１校：７００人（児童６５０人、教員５０人） 中学校モデル校１校：２７０人（生徒２２０人、教員５０人） ※対象者数については、今後の導入校拡大により、増加となる場合がある。 ※個人情報の流れは、資料５８－１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　電子図書サービスの導入に係る外部結合について

保有課（担当課）	教育支援課
登録業務の名称	電子図書サービスの導入
結合される情報項目（だれの、どのような項目か）	１　個人の範囲 区立学校児童・生徒及び教員 ２　記録項目 学校名、学年、クラス、出席番号、氏名、ニックネーム、SS0 連携用メールアドレス、閲覧項目、書誌情報、マイデスク作成物（自分で調べた情報をまとめたお気に入り機能）、検索履歴、感想コメント、ランキングコメント、ログ情報（閲覧冊数・ページ数等）、管理者氏名、管理者電話番号、管理者メールアドレス
結合の相手方	株式会社ポプラ社（ＩＳＭＳ認証取得済）
結合する理由	電子図書サービスを導入することで、児童・生徒の不読率（本を読まない児童・生徒の割合）の軽減や、授業での探究的な学習等を行うため。
結合の形態	インターネット回線を利用して、電子図書サービスとＧＩＧＡ端末、区のイントラネット端末及び校務用パソコンを接続する。
結合の開始時期と期間	令和７年４月１日から（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

電子図書サービスを利用した個人情報の流れ

区立学校 教育委員会

タブレット
パソコン
-教員用GIGA端末
-区イントラ端末
-校務用PC

児童・生徒 教員

タブレット
（GIGA端末）

【インターネット】

通信暗号化

①電子図書サービスにログインし、
児童・生徒のユーザアカウントを登録

④閲覧冊数・利用時間数・
閲覧ページ数等を収集

②電子図書を閲覧
③図書の感想を入力（任意）
（感想コメント、ランキングコメント）

・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

電子図書サービス（AWS）

対象者情報

①学校名
②学年
③クラス
④出席番号
⑤氏名
⑥ニックネーム
⑦メールアドレス
⑧閲覧項目、書誌情報※1
⑨検索履歴※1
⑩マイデスク作成物※1
⑪感想コメント※2
⑫ランキングコメント※2
⑬利用状況
（閲覧した冊数、読んだページ数、利用した時間数、読み終わった冊数、これまでに読んだページ数の累計）
⑭管理者氏名
⑮管理者電話番号
⑯管理者メールアドレス

※1　⑧～⑩については、**教員・教育委員会による閲覧不可**

※2　⑪⑫については、児童生徒が「非公開」に設定した場合は、**教員・教育委員会による閲覧不可**

【インターネット】

通信暗号化

事業者

・問い合わせ対応のための情報の取得、収集
・統計情報資料の作成・利用

・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

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。