

2018年（平成30年）6月14日

藤沢市教育委員会
教育長 平岩 多恵子 様

藤沢市個人情報保護制度
運営審議会会長 畠山 関之

図書館資料の貸出、閲覧及びレファレンスに係る
コンピュータ処理について（答申）

2018年（平成30年）5月28日付けで諮問（第925号）された図書館資料の貸出、閲覧及びレファレンスに係るコンピュータ処理について次のとおり答申します。

1 審議会の結論

藤沢市個人情報の保護に関する条例（平成15年藤沢市条例第7号。以下「条例」という。）第18条の規定によるコンピュータ処理を行うことは適当であると認められる。

2 実施機関の説明要旨

実施機関の説明を総合すると、本事務の実施に当たりコンピュータ処理を行う必要性は、次のとおりである。

(1) 諮問に至った経過

総合市民図書館、南市民図書館、辻堂市民図書館、湘南大庭市民図書館はオンラインで接続しており、業務系ネットワークとして資料検索、予約業務、貸出・返却業務、利用者管理業務、蔵書管理業務、書誌管理業務、統計・帳票管理業務、発注・受入業務を4市民図書館で共通利用している。各業務の処理を行う業務系サーバが総合市民図書館に設置されているため、オンライン処理及びシステム保守管理は総合市民図書館で行っている。

国会図書館、県立図書館、及び市内の大学図書館などがインターネットに対応したサービスを開始したため、藤沢市図書館でも1999年（平成11年）にインターネットから資料検索ができるサービスを開始し、インターネットからのアクセスを処理する情報系サーバを導入した。さらに図書館業務に使用する目的で、藤沢市図書館内にインターネット

やEメールが利用できる情報系ネットワークの構築を行った。

また、2005年（平成17年）にはインターネットから資料の予約ができるサービスを開始した。このサービスの開始に伴い、インターネットから利用者が入力するパスワード及びメールアドレスを入力処理する情報系サーバと利用者情報の登録にて作成されたデータ等を管理する業務系サーバをSNAプロトコルにより結合することについては、2004年（平成16年）11月4日付け答申135号「図書館予約システム」にて藤沢市個人情報保護制度運営審議会の承認を受けている。

図書館における利用者サービスの拡充の一環として、利用者からのレファレンス依頼をインターネット上から受け付け、Eメール及び代替手段で回答するサービスの実施に伴い、新規に個人情報の取得があることについては、2008年（平成20年）11月13日付け答申352号「レファレンス業務」にて承認を受けている。

2012年（平成24年）にシステム機器の老朽化及び保守サポート切れに伴い、全面的なシステム機器の入替えを行い、業務系サーバと情報系サーバを1台のサーバで担う構成に変更したことについては、2012年（平成24年）5月10日付け答申502号「コンピュータ処理」にて承認を受けている。

このたび、2019年（平成31年）3月にシステム機器の老朽化及び保守サポート切れに伴い、全面的なシステム機器の入替を予定している。使用する図書館システムパッケージ、機器の構成についてはセキュリティ向上を目的に次の変更を予定している。

ア 図書館システムパッケージ

現行図書館システムパッケージ「CLIS/400 総合図書館情報システム」のバージョンアップにあたる「CLIS/Ver. 3.1 統合図書館情報システム」を利用する。

また、図書館システムパッケージの変更に伴い、市民利便性の向上の観点から図書館ホームページに次のサービス機能を追加する。

(ア) 図書館ホームページに追加を予定しているサービス機能

a パスワード登録

館内 OPAC 及び WebOPAC で利用者が使用する個人用パスワードを、利用者自身が図書館ホームページから発行ができる機能

b 利用者仮登録申請

図書館ホームページから図書館カードの事前申請ができる機能

c マイライブラリ機能の「お気に入り資料」

利用者自身がお気に入り資料を登録し、登録した資料の確認ができる機能

d レファレンスの回答

館内 OPAC 及び WebOPAC のマイライブラリ機能から利用者がレファレンスの回答を確認できる機能

イ 機器の構成

現行の機器の構成は、インターネットや E メールを利用した調査、市外からの図書資料借用、及び書誌データの取得等事務の処理を主に行う情報系サーバと資料検索、予約業務及び貸出・返却業務等個人情報を扱う図書館業務の処理を主に行う業務系サーバを 1 台のサーバで担うように構成をしているが、次期の機器の構成では、情報系サーバと業務系サーバを別々のサーバに分離すると同時に、ネットワークも業務系ネットワークと情報系ネットワークを仮想分離する構成にする。

以上のことから、追加サービス機能及び機器の構成の変更について、条例第 18 条の規定に基づき、藤沢市個人情報保護制度運営審議会に諮問するものである。

(2) コンピュータ処理をする必要性について

藤沢市図書館では、図書館情報システム（業務系）によりコンピュータを利用することで、利用者サービスの拡充、業務の効率化を図っている。平成 29 年度における藤沢市図書館 4 館の主な実績件数は次のとおりである。

	登録者数 (人)	貸出者数 (人)	貸出件数 (件)	予約件数 (件)
平成 29 年度	117,795	1,137,348	2,875,266	615,471

今後も利用者サービスを展開していくにあたり、コンピュータの利用は必要不可欠である。次に挙げる「コンピュータに入力する個人情報の範囲」については、変更がなく、2012年（平成24年）5月10日付け答申502号「コンピュータ処理」にて承認を受けている。

ア コンピュータに入力する個人情報の範囲

- (ア) 住所
- (イ) 氏名
- (ウ) 電話番号
- (エ) 生年月日
- (オ) 利用者 ID
- (カ) 個人用パスワード
- (キ) E メールアドレス
- (ク) 質問者区分（一般・学生・高校生・中学生・小学生以下・その他）
- (ケ) レファレンス内容

「(ア)～(オ)」は貸出サービスの利用者、「(カ)」はインターネット予約を希望される利用者、「(キ)」は E メールでの通知を希望される利用者、「(ク)～(ケ)」は E メールを利用したレファレ

ンスサービスの利用者から提供される。

(3) 取得情報に対する安全対策及び管理基準

ア 取得した情報の取扱い

取得した情報の取扱いについては、図書館内の端末にて職員により処理が行われる。図書館情報サービスに係る業務においてコンピュータで取り扱う個人情報とは現行システムと同様であり、現行のコンピュータに保存されている個人情報については、すべてシステム機器の入替後のコンピュータ（業務系）に移行する。この個人情報の取扱いについては、藤沢市個人情報保護制度運営審議会への答申第135号、答申第352号及び答申第502号にて承認されているものである。

イ セキュリティ対策

セキュリティ対策については、答申第135号、答申第352号及び答申第502号にて承認されている現行図書館システムパッケージ「CLIS/400 総合図書館情報システム」のバージョンアップにあたる「CLIS/Ver. 3.1 統合図書館情報システム」を利用することにより確保する。「CLIS/Ver. 3.1 統合図書館情報システム」では答申第502号にて承認されている「CLIS/400 総合図書館情報システム」のセキュリティ対策を継続する。

ただし、「(1) 諮問に至った経過」で記載したとおり、図書館ホームページの追加サービス機能及び機器の構成の変更があるため、追加のセキュリティ対策を講じる。

(ア) 図書館ホームページの追加サービス機能に伴うセキュリティ対策

図書館ホームページでは、前述のとおり次の4点のサービス機能が追加される。

- ・パスワード登録
- ・利用者仮登録申請
- ・マイライブラリ機能の「お気に入り資料」
- ・レファレンスの回答

いずれも、利用者個人の端末からホームページにアクセスすることで提供されるサービス機能である。ホームページアクセスに関し、次のとおりセキュリティ対策を講じ、安全を確保する。

a 通信の暗号化

利用者端末（自宅PCやスマートフォンなど）から図書館側サーバまでの通信経路は、SSLにより暗号化され、通信の傍受・漏えい・改ざんを防ぐ。（従前より継続）

b 不法侵入の防止

インターネットから図書館ホームページへのアクセス並びにパスワード登録や利用者仮登録申請のために送信される情報は、

コンテンツを持たないリバースプロキシサーバを通じてアクセスされる。また、図書館ホームページのコンテンツは業務系サーバ内に存在しているが、専用のアクセス経路である WebOPAC 系セグメントを設けた上で、ファイアウォールの設定によりリバースプロキシサーバからのアクセスのみ許可するよう通信制限をかけることで、外部からの不正侵入による個人情報の漏えいを防ぐ。

c. プライバシー情報の職員の取扱い

個人パスワードやお気に入り資料などの利用者の機密情報・プライバシー情報は、業務サーバに登録されるが、図書館職員がシステム画面上から閲覧することはできない。(個人パスワードの扱いは従前より継続。)

(イ) 機器の構成の変更に伴うセキュリティ対策

ネットワークを業務系と情報系に仮想分離し、個人情報を含む図書館情報システムは業務系、インターネットを使用する調査業務等は情報系で行うことで、図書館情報システムはインターネット接続から分離され、個人情報の漏えいを防ぐ。なお、ソフトウェアアップデート・パターンファイル更新については、定期的実施する。

業務系ネットワーク内の端末(以下、「業務系端末」という。)では、例外的に情報系ネットワーク内の端末(以下、「情報系端末」という。)とデータ移行する場合があるため、業務系端末と情報系端末にデバイス制御の機能を導入し、不要な USB デバイスを扱えない設定にすることでセキュリティを確保する。

書誌情報の取得においては例外的に業務系端末からインターネット接続を行う必要があるが、情報系プロキシサーバを経由した間接的な情報取得並びに接続先ウェブサイトの特定の二面からの制限により、接続を必要最小限のものとする。

また、ファイアウォールにて、インターネット接続できるサーバをプロキシサーバに限定することにより、情報系端末が個別に直接インターネットに接続することはできない。

リモート保守については、VPN という接続方式を使い、仮想的に暗号化されたプライベート接続を構築することにより、セキュリティの確保を行う。

なお、利用者にインターネット閲覧を提供する利用者系ネットワークは、各図書館でインターネット回線を引いて提供するので、業務系ネットワークとは分離する。

ウ セキュリティ管理体制

「藤沢市コンピュータシステム管理運営規程」及び「藤沢市情報セ

セキュリティポリシー<基本方針>」を遵守するとともに、「藤沢市図書館情報セキュリティポリシー<対策基準>」に基づく運用を実施する。

「CLIS/Ver. 3.1 統合図書館情報システム」やコンピュータ端末等の設定については、情報システムセキュリティ管理者にて指名された情報システムセキュリティ担当者若しくは、情報システムセキュリティ管理者によって許可をうけた委託業者のみが行うこととする。

「CLIS/Ver. 3.1 統合図書館情報システム」のパスワードについては定期的に更新を行い、図書館より異動若しくは退職した職員等並びに委託スタッフのユーザーIDとパスワードは速やかに削除を行う。

職員については、異動時の研修等において、非常勤職員及び短時間雇用職員並びに委託スタッフについては研修等において守秘義務等の誓約をさせるほか、朝のミーティング、定期的な研修会を行うことにより、個人情報の保護の周知徹底を図る。

(4) 実施時期について

2019年（平成31年）3月1日

(5) 添付資料

ア 個人情報取扱事務届出書

イ 現行の図書館情報システム

ウ 次期の図書館情報システム

エ 図書館ホームページのアクセスフロー

オ 藤沢市図書館情報セキュリティポリシー<対策基準> 基本編
(改正前)

カ 藤沢市図書館情報セキュリティポリシー<対策基準> 基本編
(改正案)

(「4-(6) ネットワーク」の説明を2019年（平成31年）
3月1日の実施に伴い、下線部を改正)

3 審議会の判断理由

当審議会は、次に述べる理由により、審議会の結論のとおり判断をするものである。

(1) コンピュータ処理を行う必要性について

実施機関では、コンピュータ処理を行う必要性について、次のように述べている。

藤沢市図書館では、図書館情報システム（業務系）によりコンピュータを利用することで、利用者サービスの拡充、業務の効率化を図っている。平成29年度における藤沢市図書館4館の主な実績件数は次のとおりである。

	登録者数 (人)	貸出者数 (人)	貸出件数 (件)	予約件数(件)
平成 29 年度	117,795	1,137,348	2,875,266	615,471

このたび、2019年（平成31年）3月にシステム機器の老朽化及び保守サポート切れに伴い、全面的なシステム機器の入替を予定している。使用する図書館システムパッケージ、機器の構成についてはセキュリティ向上を目的に変更を予定している。

次期の機器の構成では、情報系サーバと業務系サーバを別々のサーバに分離すると同時に、ネットワークも業務系ネットワークと情報系ネットワークを仮想分離する構成にする。

また、市民利便性の向上の観点から、図書館ホームページにサービス機能の追加をする予定である。

今後も利用者サービスを展開していくにあたり、コンピュータの利用は必要不可欠である。

以上のことから判断すると、コンピュータ処理を行う必要性が認められる。

(2) 安全対策について

実施機関では、次のような安全措置を講じている。

ア 取得した情報の取扱い

取得した情報の取扱いについては、図書館内の端末にて職員により処理が行われる。図書館情報サービスに係る業務においてコンピュータで取り扱う個人情報と現行システムと同様であり、現行のコンピュータに保存されている個人情報については、すべてシステム機器の入替後のコンピュータ（業務系）に移行する。この個人情報の取扱いについては、藤沢市個人情報保護制度運営審議会への答申第135号、答申第352号及び答申第502号にて承認されているものである。

イ セキュリティ対策

セキュリティ対策については、答申第135号、答申第352号及び答申第502号にて承認されている現行図書館システムパッケージ「CLIS/400 総合図書館情報システム」のバージョンアップにあたる「CLIS/Ver. 3.1 統合図書館情報システム」を利用することにより確保する。「CLIS/Ver. 3.1 統合図書館情報システム」では答申第502号にて承認されている「CLIS/400 総合図書館情報システム」のセキュリティ対策を継続する。

ただし、「(1) 諮問に至った経過」で記載したとおり、図書館ホームページの追加サービス機能及び機器の構成の変更があるため、追加のセキュリティ対策を講じる。

(ア) 図書館ホームページの追加サービス機能に伴うセキュリティ対

策

図書館ホームページでは、前述のとおり次の4点のサービス機能が追加される。

- ・パスワード登録
- ・利用者仮登録申請
- ・マイライブラリ機能の「お気に入り資料」
- ・レファレンスの回答

いずれも、利用者個人の端末からホームページにアクセスすることで提供されるサービス機能である。ホームページアクセスに関し、次のとおりセキュリティ対策を講じ、安全を確保する。

a 通信の暗号化

利用者端末（自宅PCやスマートフォンなど）から図書館側サーバまでの通信経路は、SSLにより暗号化され、通信の傍受・漏えい・改ざんを防ぐ。（従前より継続）

b 不法侵入の防止

インターネットから図書館ホームページへのアクセス並びにパスワード登録や利用者仮登録申請のために送信される情報は、コンテンツを持たないリバースプロキシサーバを通じてアクセスされる。また、図書館ホームページのコンテンツは業務系サーバ内に存在しているが、専用のアクセス経路であるWebOPAC系セグメントを設けた上で、ファイアウォールの設定によりリバースプロキシサーバからのアクセスのみ許可するよう通信制限をかけることで、外部からの不正侵入による個人情報の漏えいを防ぐ。

c プライバシー情報の職員の取扱い

個人パスワードやお気に入り資料などの利用者の機密情報・プライバシー情報は、業務サーバに登録されるが、図書館職員がシステム画面上から閲覧することはできない。（個人パスワードの扱いは従前より継続。）

(イ) 機器の構成の変更に伴うセキュリティ対策

ネットワークを業務系と情報系に仮想分離し、個人情報を含む図書館情報システムは業務系、インターネットを使用する調査業務等は情報系で行うことで、図書館情報システムはインターネット接続から分離され、個人情報の漏えいを防ぐ。なお、ソフトウェアアップデート・パターンファイル更新については、定期的実施する。

業務系端末では、例外的に情報系端末とデータ移行する場合があるため、業務系端末と情報系端末にデバイス制御の機能を導入し、不要なUSBデバイスを扱えない設定にすることでセキュリティ

ィを確保する。

書誌情報の取得においては例外的に業務系端末からインターネット接続を行う必要があるが、情報系プロキシサーバを経由した間接的な情報取得並びに接続先ウェブサイトの特定の二面からの制限により、接続を必要最小限のものとする。

また、ファイアウォールにて、インターネット接続できるサーバをプロキシサーバに限定することにより、情報系端末が個別に直接インターネットに接続することはできない。

リモート保守については、VPN という接続方式を使い、仮想的に暗号化されたプライベート接続を構築することにより、セキュリティの確保を行う。

なお、利用者にインターネット閲覧を提供する利用者系ネットワークは、各図書館でインターネット回線を引いて提供するので、業務系ネットワークとは分離する。

ウ セキュリティ管理体制

「藤沢市コンピュータシステム管理運営規程」及び「藤沢市情報セキュリティポリシー<基本方針>」を遵守するとともに、「藤沢市図書館情報セキュリティポリシー<対策基準>」に基づく運用を実施する。

「CLIS/Ver. 3.1 統合図書館情報システム」やコンピュータ端末等の設定については、情報システムセキュリティ管理者にて指名された情報システムセキュリティ担当者若しくは、情報システムセキュリティ管理者によって許可をうけた委託業者のみが行うこととする。

「CLIS/Ver. 3.1 統合図書館情報システム」のパスワードについては定期的に更新を行い、図書館より異動若しくは退職した職員等並びに委託スタッフのユーザーID とパスワードは速やかに削除を行う。

職員については、異動時の研修等において、非常勤職員及び短時雇用職員並びに委託スタッフについては研修等において守秘義務等の誓約をさせるほか、朝のミーティング、定期的な研修会を行うことにより、個人情報の保護の周知徹底を図る。

以上のことから判断すると、安全対策上の措置が施されていると認められる。

以上に述べたところにより、コンピュータ処理を行うことは適当であると認められる。

以 上