デジタルネットワーク環境における図書館利用のプライバシー保護ガイドライン

公益社団法人日本図書館協会
2019 年 5 月 24 日

1. はじめに

このガイドラインは、デジタルネットワーク環境において、図書館利用のプライバシーを保護するために図書館が取り組むべき具体的内容を示すものである。

日本図書館協会は 1979 年に「図書館の自由に関する宣言」（以下、「図書館の自由宣言」）の主文第 3 に「図書館は利用者の秘密を守る※1。」ことを加えて改訂した。1980 年代に図書館にコンピュータが導入され始めると、1984 年にはプライバシー保護の指針として「貸出業務へのコンピュータ導入に伴う個人情報の保護に関する基準※2」（以下、「基準」）を定め、この「基準」についての委員会見解を公表※3した※4。

その後、1990 年代には日本でもインターネットが普及して ICT※5もめざましく進み、図書館もその環境の中でコンピュータによる貸出を行うようになっていった。現在の図書館情報システムにおいてもインターネットを活用したネットワーク化は不可欠なものであり、データを管理するサーバの外部化が効率性、経済性を理由として進んできた。このような環境のもとで図書館サービスを実施するには、1984 年の「基準」では対応しきれない面も顕在化してきた。例えば、従来、資料が返却されれば消去してきた利用履歴を、サービスに積極的に活用しようとする動きもあり、利用者のプライバシー保護の観点からの対応を迫られている。上記で述べたような「基準」では対応しきれない部分について、このガイドラインにおいて修正した指針を提示した。

コンピュータ性能の飛躍的向上とインターネットによるネットワーク環境により、大量なデータの迅速な処理が可能となった反面、ひとたび情報流出があると大きな被害をもたらすことになる。国際貿易上の要請※6もあり、個人情報についてはあらゆる機関に於いて法律及び条例等（いわゆる個人情報保護法制）で厳しく保護されるようになった。それでも不注意、あるいは故意の情報流出事件は後を絶たない。これらに対応するためには、図書館業務での日常的な点検と共に、職員一人ひとりがプライバシー保護に対する意識を高めること、図書館がプライバシー取扱方針を明らかにして利用者への理解を求めることが必要である。どのような状況でも、図書館は図書館利用のプライバシー保護に責任をもたなければならない。また、このガイドラインは、館種※7・運営形態にかかわらず適用されなければならない。

※1 プライバシー保護と同義であり、今日では積極的プライバシー権の保障も意味する。
※2 1984 年 5 月総会決議
※3 1984 年 10 月
※4 日本図書館協会ホームページの「図書館の自由委員会」ページに掲載
※5 Information and Communication Technology（情報通信技術）の略
※6 OECD8 原則（1980 年 OECD 理事会勧告）や EU データ保護指令（1995 年）、現在は EU 一般データ保護規則（2016 年）で運用
※7 公共図書館のみならず、学校図書館、大学図書館、専門図書館等のすべての館種に適用される。

2. プライバシー保護の重要性

図書館は、日本国憲法第 21 条ないし国際人権規約 B 規約（市民的及び政治的権利に関する国際規約）第 19 条が定める知る自由をすべての人に保障するために、自由な情報アクセスや読書ができる環境を提供する機関である。基本的人権のひとつとしての知る自由を保障する図書館が、図書館利用者のプライバシーを保護することはサービスを遂行するために必要不可欠な義務である。

「図書館の自由宣言」では、主文第 3 で「図書館は利用者の秘密を守る。」と宣言している。図書館は、利用者の内心やセンシティブ（機微）情報といったプライバシーを、個人情報保護に関する法及び条例で規定されるずっと以前から大切に守ってきた。これは憲法第 13 条の個人として尊重される権利、第 19 条の思想及び良心の自由の権利として保障されている。

専門職としての図書館員が立脚すべき規範として制定した「図書館員の倫理綱領」においても、主文第 3 で「図書館員は利用者の秘密を漏らさない。」と規定している。図書館利用者へのサービス提供において、利用者のプライバシーの権利を守ることは、図書館に従事するすべての人びとに課せられた責務である。

3. どんな場面で「個人情報」「利用情報」が収集されるか

図書館は、提供するサービスのために必要な、個人を識別する情報（以下、個人情報）として、氏名、住所などの情報を収集する。個人情報と利用情報の収集は、資料管理が目的である。どのような情報をどのような目的で収集して利用するかについては、事前に利用者に提示して利用者の同意を得る必要がある。個人情報を収集するにあたっては、図書館サービスを提供するための必要最小限の項目とする。

個人情報と利用情報は、次のような場面で収集され、ログ※8も記録されて蓄積される。

（1）図書館システム

ア　図書館利用のための個人情報の登録

利用者 ID、氏名、住所、電話番号、生年月日、メールアドレス、在勤・在学の情報

イ　個人情報と結びついた利用情報

貸出・返却・延滞・督促・予約・リクエスト・レファレンス記録

ウ　来館の記録

入退館及び滞在中の情報

施設、閲覧席等の利用

（2）図書館内の OPAC（利用者用検索機）

ア　利用者個人と結びつきうる利用者 ID を含む情報を用いたログイン中の記録

（3）閲覧※9用パソコン（以下、館内 PC）の利用

ア　利用記録と閲覧履歴

イ　Web サイトへのアクセス

フィルタリングソフトへのログの蓄積

※8 OS やソフトウェア、データベースに対する更新処理を記録したもの。アクセスログ、エラーログ等
※9 インターネット・データベース等の図書館が提供するサービス利用

リンク先へのログの蓄積
各通信機器への通信ログの蓄積

（4）図書館 Web サイトの利用

ア　利用者 ID でのログイン中の記録

（5）図書館が提供するインターネット回線※10の利用

4. 収集した情報の管理

図書館が管理する個人情報と利用情報は、図書館が提供するサービスのために収集する。図書館は、どのような個人情報と利用情報が収集されるかを把握し、必要最小限の情報を必要最短期間保持することを原則としなければならない。

図書館は、その原則に基づいた収集方法、管理方法や削除時期などについて定め、公開する。

（1）個人情報と利用情報（以下、利用者情報※11）の管理

ア　利用者情報は永続的に保管すべきではない。

イ　利用者情報を含む記憶媒体や文書の保管方法を定め､保管期間を終了したデータは速やかに消去する。

ウ　利用者情報は図書館外に持ち出さない※12。

エ　個人情報と利用情報との結びつきは、貸出や予約等の利用終了後、保管期間を定め確実に解除する。

オ　統計上必要な情報を残す場合は個人情報を匿名化し利用情報との結びつきを切る。

カ　資料管理の範囲を超える情報の収集や管理を伴うサービス（利用履歴活用サービス、マイページ、読書通帳など）については、利用者のプライバシー保護を最優先に考え、導入する場合には図書館内で慎重に検討し、十分な安全対策を講じる必要がある。

キ　資料管理の範囲を超える情報の収集や管理を伴うサービスは利用者にメリット・デメリットを十分説明して理解を得たうえで、サービスを希望する利用者のみに提供する。

ク　サービス中止の希望は速やかに履行し､保存していた利用記録は完全に消去しなければならない。

（2）パスワード・個人情報の管理

ア　パスワードは平文※13ではなく、暗号※14化するなどの対策を講じて保管しなくてはならない。

イ　個人情報は最新･最適なシステムを使って外部に流出しないよう、管理しなければならない。

ウ　クラウド※15ベースで保管されている利用者情報も、十分な安全対策を講じなければならない。

※10 Wi-Fi™ に代表されるような無線 LAN 接続環境の提供 等
※11 図書館の自由宣言では、読書事実と利用事実に切り分けている。
※12 クラウドベースで保管される利用者情報については、後掲「6. 外部とのネットワーク」を参照。
※13 秘匿化・隠蔽化の処理が何も行われていない、そのままのデータ。
※14 平文の一般的な反義語。ID 認証では復元化が必須でないため、通常ハッシュ化技術が使用される。
※15 クラウドストレージ（外部にあるサーバにファイルを置く）サービスのこと。災害に強いなどの利点がある。

（3）ログの管理

ア　システムに残るログには、統計等に使用するアプリケーションログのほか、システムの動作を記録するシステムログ、システム不具合時にデータを復旧させる目的のバックアップログがある。

イ　各図書館では、ログの管理と運用を定める。その保管規則に従い、記録媒体の消去・廃棄を行わなければならない。

（4）第三者との共有、第三者によるモニタリング

ア　図書館は、Web サイト・ OPAC ・ディスカバリーサービス※16等、図書館利用者向けの外部企業による検索サービス等に含まれる外部プログラムへのリンク等により、利用者情報が収集されていることを認識し、そのことを利用者に説明しなければならない。

イ　利用者の同意や裁判所の命令なしに、図書館利用者の利用者情報に関するデータを第三者に提供してはならない。

（5）図書館内の利用者用インターネット端末に残る利用履歴、Web サイトの追跡への対応

ア　一人ひとりの利用終了時に履歴・ cookie※17・パスワードなどのすべてのデータが消去されるように設定しなければならない。

（6）管理権限の限定

ア　利用者情報へのアクセス、統計情報や Web 解析の処理は、権限を付与された特定の図書館員のみに限られるべきである。

イ　統計情報を公開するときや Web 解析を行う場合、個人を特定できる情報を匿名化しなければならない。

5. 利用者による自己情報へのアクセスとコントロール

利用者は、自分の個人情報にアクセスしコントロールする権利を持つ。このことは、利用者が自分の個人情報が正確に管理されているかを確認し、適切な図書館サービスを受けるために必要である。

（1）図書館は、利用者に関してどのような情報を収集し、どのような目的で利用し、どのくらいの期間保管するかについて、利用者が容易に知ることができるようにする必要がある。

（2）利用者が自分の個人情報にアクセスできるようにするとともに、その方法についてわかりやすい案内をする必要がある。

（3）利用者から個人情報が不正確だという指摘があった場合は正しい情報に修正する。

（4）貸出履歴や検索履歴などを活用するサービスを導入する場合は、利用者がサービスの利用について希望者のみ選択できる方式（オプトイン※18）にしなければならない。選択の際には、どれくらいの情報がどのように利用されるか、どのような危険性があるかについて利用者に十分に説明するとともに、利用者がいつでもその説明を見られるようにする。また、利用者の希望でいつでもやめることができるようにし、そのときはサービスを受けていた期間に収集した情報を破棄する。

※16 OPAC、電子ジャーナル、データベース等を同一のインターフェイスで検索できるサービス
※17 Web サーバとの通信で、Web ブラウザに保存される情報。ユーザ識別やセッション管理に利用される。
※18 事前にユーザーの承諾を得ること。反義語はオプトアウトで事後の拒否による除外を示す。

6. 外部とのネットワーク

館内 PC や図書館のサーバーシステムは、インターネット環境下では、常に外部からの脅威に晒されており、オンラインによるセキュリティ対策が必須である※19。

システムの安定運用にはログの取得・管理は必須であり、ブラウン方式で貸出を行っていた時代のように、紐づけの解除後にその痕跡を全く残さないことは不可能に近い。

危機管理の観点から言えば、情報漏えいの危険性は、どんなに高度な対策を取ったとしてもゼロにはならない。図書館利用者との信頼関係を担保する上では、必要かつ妥当な対策を常に検討し、実施していく必要がある。

(1) クラウドシステムによる外部化

ア　システムの高度化により、館内でシステムを運用するより、クラウドシステム導入による外部化が、セキュリティ対策上も優位である場合があり得る。運用者の選定にあたっては、プライバシー保護やセキュリティ対策及び図書館業務への理解などの観点から、それぞれの優位性・課題を図書館が主体的に検討し、決定する必要がある。

イ　クラウドシステム導入にあたっては、以下のような視点が重要である。

(ｱ) システム運用業者に、公務員と同等の厳格な守秘義務を課す。

(ｲ) すべてのデータの所有者は図書館である。

(ｳ) 通信の適切な暗号化を担保する。

(ｴ) 個人情報・利用情報の第三者への提供は、匿名化処理を行っても許可しない。

(ｵ) 日本法を準拠法とし日本国内の裁判所を管轄裁判所とするよう留意する。

ウ　システム運用業者に捜査情報提供の要求があったときは、速やかに図書館への報告を求める。捜索差押許可状の提示がない場合は情報の提供を認めない。

(2) 外部ネットワークの利用

ア　OPAC や図書館ホームページで、外部サイトへのリンクを提供する場合、そのサイトのプライバシー・ポリシー等を確認し、利用者情報の取扱いを認識しておく。必要に応じてその内容を利用者に提示することは重要である。

イ　利用者情報では閲覧履歴、cookie、ID ・パスワードなど利用者の外部サイト利用の全ての痕跡が対象である。

(3) インターネットによる情報発信

ア　インターネットを利用した情報提供サービスを行う場合、図書館システム内部のアプリケーションやスクリプト※20等が、図書館の意図しない利用者情報を収集しないよう十分な確認が必要である。

イ　ログインを必要とするサービスを提供する場合には、プライバシー・ポリシーを公開し、利用者情報の管理には細心の注意を払う必要がある。

(4) 共用カードによる情報共有

ア　国や自治体が発行するカード※21、民間ポイントカード、学生証等を図書館カードとし

※19 このような状況下で、プライバシー保護やセキュリティ対策を意図してネットワークから切り離すことは現実的でない。

※20 特定の機能を記述する簡易なサブプログラム

※21 マイナンバーカード、住民基本台帳カード等

ても利用する場合、一定の利用者情報が共有される※22ことが前提であると認識しなければならない。

イ　共用カードを図書館カードとして利用する場合、利用者の同意が前提である。

ウ　共用カードを希望しない利用者には、専用の図書館カードを選択できるよう準備する。

エ　学校・大学図書館及び企業内図書館などで、学生証・職員証などを図書館カードとして共用せざるを得ない場合、プライバシー保護について十分な対策を講じた上、その危険性を周知する。

7. 図書館員のプライバシー意識と図書館の体制

このガイドラインを遂行するためには、図書館員のプライバシー保護に対する意識を高めるとともに、図書館が図書館利用のプライバシー保護に責任を持つことが大切である。図書館を運営委託（指定管理者等）している場合においても同様である。

図書館利用のプライバシー保護及び個人情報開示に関する責任者である図書館長は、図書館についての専門的見識を有する司書有資格者であることが望ましい。

(1) 図書館は、全ての業務とサービスについて、独自にプライバシー・ポリシーを策定しなければならない。策定の際には、JIS、ISO 規格※23や自治体のプライバシー・ポリシーに留意する。

(2) 図書館は自館のプライバシー・ポリシーを実施するための効果的な方法を構築し維持しなければならない。各業務とサービスが図書館のプライバシー・ポリシーに適合することを確認するために、定期的にプライバシー監査を受ける。

(3) 図書館で働く全ての人は、職務内容に応じてプライバシーや情報セキュリティに関する研修を計画的、継続的に受ける。

(4) 個人情報や利用情報漏洩等の緊急事態が発生した場合には、その事実を公開し、速やかに対応する。

（公益社団法人日本図書館協会　図書館の自由委員会 作成）

※22 どんなサービスであれ、利便性の向上は情報セキュリティ上の危険性を増加させる。

※23 JIS Q 15001（個人情報保護マネジメントシステム-要求事項）、ISO/IEC 27001（情報セキュリティマネジメントシステム）等