【大学図書館員のための個人情報保護チェックシート：解説編】

＜組織体制について＞

1-3. 学内の個人情報保護責任者・委員会の設置

→個人情報保護（管理）責任者の選任は、文部科学省告示第百六十一号　第三（四）「事業者が講ずべき措置の適切かつ有効な実施を図るための指針となるべき事項」で述べられている。組織内で統一的に個人情報を管理するため、委員会などの設置が必要となる場合もあると考える。できれば分校や各部署など、セクションごとに責任者や窓口を設置することが理想である。

参考情報：文部科学省告示第百六十一号　第三（四）「事業者が講ずべき措置の適切かつ有効な実施を図るための指針となるべき事項」

1-5. 組織内での個人情報保護教育

→個人情報の取扱いに関して職員としての自覚を持ってもらい、大学または図書館としての個人情報の管理方針について共通認識を持つための啓発活動や職場研修が必要となってくる。他にも個人情報管理責任者向け、および個人情報を取扱う職員や従業者向けなど、担当者レベルの実務研修を実施することも考えられる。学内だけでなく、学外機関の研修の機会があれば活用するのもよい。

参考情報：文部科学省告示第百六十一号　第三（五）

1-6. 対応マニュアルの策定

→漏洩に関する窓口対応を、内部での報告ルートを含め、マニュアル化しておくとよい。情報漏洩についての対応は、「問題が起こったら」編を参照。

1-10. 危機管理全般、漏洩後の対応に関する外部コンサルティングの利用や保険商品

→富士通株式会社は「個人情報保護法対策簡易評価」サービスを提供しており、個人情報の取扱いの評価や、対策についてガイダンスを提案している。また、「学校総合賠償責任保険」（損保ジャパン提供）のように、個人情報の漏洩を含む学校の管理ミスに対する賠償金や訴訟費用を補償する保険が販売されている。他にも、個人情報について適切な保護措置を講ずる体制を整備している事業者を認定するプライバシーマーク制度といった第三者機関からの審査・認定制度がある。

　こうした外部コンサルティングや保険商品についても調査を行い、個人情報保護への対応策としての選択肢となり得るか検討しておいてもよい。これらの多くは、図書館という部局単位ではなく学校法人または大学全体での申請または契約となるので、学内の方針の下で検討することになる。

参考情報：

1．富士通株式会社「個人情報保護法対策簡易評価」チェックリスト

2．株式会社 NTT データ経営研究所、株式会社メトロジー

「個人情報保護法対応 Web 簡易診断サービス」

個人情報保護法への対応状況をインターネット上で簡易に自己診断するためのサービス

http://www.keieiken.co.jp/consulting/itm/security_survey/

3．損保ジャパン「学校総合賠償責任保険」の販売について（2005 年 7 月 11 日付け）

4．財団法人日本情報処理開発協会　プライバシーマーク制度　http://privacymark.jp/

＜図書館で扱う個人情報の利用目的・収集・保存について＞

2-11. 目的の範囲内で必要な情報のみ収集

→氏名・学籍番号・住所・電話・E メールアドレス・所属機関および勤務先など、業務において必要不可欠な情報だけに厳選し、申込書の不要な項目を省く方が望ましい。

2-12. 各種申込書は単票形式

→連記形式（ノートなど）は、次以降の記入者など、他の利用者への個人情報の漏洩の可能性があるため、単票形式にし、利用者の目に触れない場所に保管する。

＜図書館独自で収集した各種申込書および個人情報＞

※　各種申込書は下記のものが考えられる。

- 図書館利用登録申込書（学内者用）　→＊a)
- 住所変更届　→＊a)
- 文献複写申込書
- 相互貸借申込書
- 購入希望申込書
- 参考質問票
- 図書館利用登録申込書（卒業生・外部利用者）
- 資料請求票
- 利用状況確認画面におけるパスワードの変更申請書　→＊b)
- 施設・設備（部屋・OA 機器など）利用申込書

※　各種申込書以外では下記のものが考えられる。

- 入館ゲートのログ
- 防犯カメラのデータ　→＊c)
- 投書用紙
- アンケート調査用紙

＊a)図書館利用登録者の情報（学内の学生・教職員用）、住所変更届について

→図書館独自で収集した情報か、大学で収集した情報かによって、管理方法・責任が異なる。学内他部署が管理する場合、LAN などデータでの連携を図ることにより、紙媒体での漏洩を防ぐ。また、学生・教職員全員に E メールアドレスを与え、E メールでの連絡ができる環境を作ることにより、呼出（掲示・電話伝言・郵送など）で第三者に情報が漏洩する内容が減少する。

＊b)利用状況確認画面におけるパスワードの変更申請書

→電子情報取扱い者を限定し、厳重な管理のもとで閲覧する。また、廃棄する際にはデータが復元できないよう、リース返却時にも漏洩しない方法をとる。

＊c)防犯カメラのデータ

→資料の盗難や破損などを防ぐ目的だけではなく、空席状況などを確認する目的と兼ねて、設置する方法もある。利用者に“監視されている”という意識を持たせず、不快感を与えないよう配慮もした方がよい。

※個人情報は下記のものが考えられる。

- 氏名
- 学籍番号
- 住所
- 電話番号
- 生年月日
- E メールアドレス
- 帰省時連絡先
- 利用履歴
- パスワード

・所属機関（卒業生・外部利用者の場合の勤務先など）
・その他

＜委託業者との取り決めについて＞

3-2. 委託業者との契約

→JIS Q 15001 においては、事故時の責任分担についても契約書に明記するべきとされている。情報漏洩した場合の賠償について、契約書に「全額」「すべて」と明記されている例もあるが､全ての被害額を想定することは難しいとされ､現実的ではないと言われている。委託先と協議の上、無理のない契約を交わすことが必要だと言える。裁判費用および損害賠償費用の負担について明記することも一つの手段と言える。

参考情報：直江とよみ「やさしく読む『個人情報保護法』」

http://www.atmarkit.co.jp/fsecurity/rensai/privacy01/privacy01.html

3-3. 委託業者の個人情報保護の取扱い

→個人情報保護法第 22 条において、委託先への監督義務がうたわれている。契約時に大学で作成した個人情報保護方針と同等のものを遵守することを契約として明記する。

＜相談窓口について＞

4-1. 苦情・相談窓口の設置

→相談窓口は、広く周知する必要がある。館内にポスターなどを掲示したり、ホームページにも掲載しておくとよい。

＜呼出・連絡（督促･購入希望･予約本･落し物･レファレンス関係など）＞

個人情報の漏洩を防ぐために、より安全性の高い方法で呼出を行えないか検討することも必要である。

5-1. 掲示による呼出

→目的や呼出内容の詳細を記載している場合、特定の利用者の嗜好が第三者に漏洩する可能性がある。呼出内容の詳細を記載せずに氏名だけ掲示し､「下記の方はカウンターまでおこしください」という方法をとる。

5-2. 電話連絡での伝言

→転居・長期不在（留学）などにより、長期延滞中の本人に連絡がとれない場合に、本人以外に書名を伝え返却を依頼する場合がある。第三者提供にあたるため、予め「家族などに伝言をする可能性がある」と目的を明示しておく必要がある。

5-3. 郵送

→ハガキの場合は､第三者から見える個所に目的を明記していないか。タイトルや資料 ID は、OPAC などの２次資料によりタイトルや内容を特定できるため、伏せる必要がある。封書やシークレット対応ハガキに切り替え、本人のみに目的を伝える。

※　呼出事項には下記のものが考えられる。

- 督促
- 購入希望
- 予約本
- 落し物
- 文献複写・資料借用
- その他

＜蔵書としての名簿類（市販されていない学内配布物的な名簿類）の管理について＞

6-1. 学内で作成された名簿類の公開

→個人情報保護法は、公知・非公知の別を問わず「個人情報」に対して義務規定が適用されるため、掲載にあたって本人が同意していても第三者提供の制限を受ける。私立大学の図書館における資料の提供については、学術研究を目的で利用する場合には、個人情報取扱い事業者の義務は適用されない。よって、閲覧制限を行う必要はない。ただし、図書館内部における個人情報の取扱い全てが学術研究目的とは限らないので、あくまで、該当資料の利用に限定して義務規定の適用が除外されるにすぎない。また、プライバシーを侵害する恐れがある資料については、個人情報保護ではなく、プライバシーの権利の保障のために、閲覧を制限することがあり得る。

学内で作成された名簿などは、利用目的の範囲内で取扱うことが第一である。市販の名簿と同様の扱いではなく、内部資料として取扱う方が適切である。第三者提供の制限は、本人からの求めに応じて第三者への提供を停止する「オプト・アウト」に応じることで、本人の同意なしに第三者に提供することもできる。掲示や公表などを行うにあたって「オプト・アウト」の処置を講ずる方法もある。

※名簿類（蔵書）は下記のものが考えられる。

- 卒業アルバム
- 卒業生名簿
- 在校生名簿
- 職員名簿
- その他

＜寄贈資料について＞

7-1. 寄贈者名の記載

→トラブル防止のため、予め寄贈者に名前を記載することを伝えるべきである。

7-2. 寄贈者名のデータ化

→今後は、何らかの形で寄贈者名を残してある図書館においては、その情報が本当に必要かどうかを検討の上、不要であれば寄贈者名は残さない方が賢明だろう。

7-3. 寄贈者名を利用者が閲覧できるデータに入力しない

→寄贈者名を図書に記載したり、利用者が閲覧できるデータに入力したりすると、他の利用者に寄贈者名を知らせることになる。個人情報保護対策において、必要以上の情報を収集しないことは大変重要なことである。

＜システム関連について＞

8-1. 端末類の検索履歴などの記録消去設定

→パスワードを残さないように、ブラウザを設定する。ウィンドウを閉じたり、ログアウトをすることで、記録や履歴が消えるように設定する。設定した上で、利用者へ広報することが大切である。

8-2. 各種申し込みフォームのセキュリティ

→取扱い、利用目的に関する文言を記載する。セキュリティの強化・暗号化。

8-3. システム面における監査

※システムに関する監査には、下記のような内容が挙げられる。

- ファイアウォール、サーバへのアクセス制御、サーバやルータの設定など、外部進入に対するセキュリティポリシーに基づいた運用がなされているか。
- 不正アクセスがないか、アクセスログのチェックを定期的に実施しているか。
- 類似アタックテストを定期的に行い、外部からの不正アクセス対策を実施しているか。
- 脆弱性の情報を収集し、適切なパッチを適用しているか。
- （データが破壊された時の対策として）バックアップは適確に行われているか。

参考情報：「学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」解説

私立大学を取り巻く諸情勢資料集（平成 17 年度第１版）平成 17 年 7 月　日本私立大学協会

8-4. Ｅメールのメールボックスやアドレス帳の管理、保存年数

→アドレス変更の対応や、メール受送信箱の管理などの管理者を決め、メール保存の年数・件数などを設定しておく。自宅への転送を行っている場合は、転送期間を限定し、漏洩しないようにする。

8-5. 業務用端末へのアクセス権限（端末設定）

→例えば、従事する業務ごとや、アルバイト／業務委託／専任職員別に個人情報に対する権限のレベルが異なるＩＤ／ＰＷを設ける。

8-6. 個人情報のアクセス権限（スタッフ）

→図書館スタッフ内での権限を差別化する。例えば、管理職のみや閲覧担当のみが個人情報を管理し、個人情報の盗み見・データの改ざん・不必要な情報の閲覧・漏洩を防ぐ。

＜電子的利用状況・貸出履歴の開示について＞

9-1. 利用状況（貸出・予約状況など）の開示

→利用者が直接閲覧する場合、利用者全員へ広報し、利用を徹底させる必要がある。パスワードの管理と変更、ログアウトなどを習慣づけさせる。ログアウトし忘れた場合は自己責任を了解してもらうようにする。

9-2. 貸出履歴の開示

→個人情報からの視点から見て履歴は一切残さないという方法が理想的である。しかし、現状では返却トラブルなど業務上の処理などで必要なため、貸出履歴を保存している図書館は多い。『図書館の自由に関する宣言(1979)』では、「貸出記録は、資料が返却されたらできるだけすみやかに消去しなければならない」と主張しているが、個人情報保護法に直接違反する訳ではない。

６ヶ月以内に消去している個人データは開示の求めの対象にならないが、個人データを６ヶ月を超えて保持していると「保有個人データ」となり、開示要求・訂正・停止などの要求に対応することが義務化された。利用者から要求があった場合は本人を確認した上で開示しなければならない。

万一スタッフが貸出記録を見る場合は、トラブルが起こった場合などに履歴を確認することがあると予め了解をとっておく必要がある。その場合は、専任スタッフが受けることが望ましい。しかし、図書館スタッフ（第三者）が嗜好・趣味を閲覧できることは、利用者に不快感をもたらし、プライバシーの侵害にもあたるため、今後は図書館ポータルサイトなどで利用者が直接閲覧できるようにしていくべきであろう。

＜内部的事項について＞

10-1. **過剰に個人情報が記載されている職員証の着用**

→職員証（身分証明書）の場合は、スタッフの生年月日なども記載している場合もあり、図書館専任スタッフの個人情報を守るにはふさわしくない。業務委託やアルバイトなどを含め、フルネームではなく、姓のみを表記した名札にするなど工夫する必要がある。

10-2. **図書館スタッフの連絡先一覧・出勤簿などの管理**

→委託スタッフ・パートタイマー・学生アルバイトの管轄は、図書館か他部署か（総務・人事・学生課など）で管理方法が変わってくる。カウンター周りに連絡先・出勤簿が放置されている場合は、施錠できる場所や別の部屋などで保管する必要がある。

構内各部署の責任者名一覧の管理も同様であり、事務室内での管理にも注意を払い、コピー制限など流出を防ぐ必要がある。

【問題が起こったら・・・：解説編】

＜問題発生後、至急対応すべき項目（第一段階）＞

A-1. 漏洩継続の阻止

→出元が学内サーバの場合は、サーバの停止措置権限など、予め取り決めておくとよい。

A-3. 迅速な広報対応（謝罪など）や主務官庁への報告

→大学の代表者または責任者が行い、情報漏洩の事実がある旨を伝え、謝意を表明する。以降、情報の公表についても他の人が見解を述べることは慎む。

A-4. 個人情報が漏洩した原因と結果の究明

→原因究明と報告を行う対応チームを作ることも考えられる。

A-8. 情報管理違反行為に対しての法的責任への対処

→漏洩は（漏洩元の組織に対する）民事訴訟の対象にもなり得る。漏洩行為や管理義務違反については、刑事罰の対象となる。

参考情報：日本図書館協会図書館経営委員会危機・安全管理特別検討チーム　「こんなときどうするの？－利用者と教員のための図書館の危機安全管理　作成マニュアル－」2004 年　社団法人図書館協会

A-9. 個人情報が漏洩した原因と今後の対策

→情報漏洩についてスタッフや従業者への報告を行う。原因究明後、個人情報管理方針や管理方法について見直しを行い、不十分な個所があれば内容を修正する。二度と同じ問題が発生しないよう、新しい情報管理方法やガイドラインに基づいて職場研修を行う。

＜問題発生後、至急対応すべき項目（第二段階）＞

B-3. 危機管理全般、漏洩後の対応に関する外部コンサルティングの利用や保険商品

→富士通株式会社は「個人情報保護法対策簡易評価」サービスを提供しており、個人情報の取扱いの評価や、対策についてガイダンスを提案している。また、「学校総合賠償責任保険」（損保ジャパン提供）のように、個人情報の漏洩を含む学校の管理ミスに対する賠償金や訴訟費用を補償する保険が販売されている。他にも、個人情報について適切な保護措置を講ずる体制を整備している事業者を認定するプライバシーマーク制度といった第三者機関からの審査・認定制度がある。

　こうした外部コンサルティングや保険商品についても調査を行い、個人情報保護への対応策としての選択肢となり得るか検討しておいてもよい。これらの多くは、図書館という部局単位ではなく学校法人または大学全体での申請または契約となるので、学内の方針の下で検討することになる。

参考情報：

1．富士通株式会社「個人情報保護法対策簡易評価」チェックリスト

2．株式会社 NTT データ経営研究所、株式会社メトロジー

「個人情報保護法対応 Web 簡易診断サービス」

個人情報保護法への対応状況をインターネット上で簡易に自己診断するためのサービス

http://www.keieiken.co.jp/consulting/itm/security_survey/

3．損保ジャパン「学校総合賠償責任保険」の販売について（2005 年 7 月 11 日付け）

4．財団法人日本情報処理開発協会　プライバシーマーク制度

http://privacymark.jp/