

# 個人情報保護の課題と対応

## —— 本校の場合 ——

室 岡 和 彦

### 1. 課 題

平成17年4月から個人情報保護法が施行され、学校における個人情報の扱いについて罰則を含むルールが明文化された。その背景には、管理している個人情報の漏洩や不十分な管理体制などがあげられる。一方、個人情報の管理等について、ともすれば過剰な反応が見られる。本校における個人情報保護の課題と解決方法は、大学のもとで附属学校園全体が関わる必要がある。

附属学校園が扱う情報は、IT化の中で大幅な見直しを迫られている。その課題は、次のようにまとめられよう。

#### (1) 管理する情報と管理方法の不明確さ

学校が扱う個人情報の収集・保管・更新・破棄などの方法、WPなどへの公開、在学中・卒業後・入学前の生徒やその保護者から要請があった場合の開示について規程を定め、運用をする必要がある。

#### (2) 情報管理の教育

教職員が共通認識をもつべき情報管理のマニュアルがなく、情報の扱いについての教育もなされていない。生徒や保護者向けの広報と教育も必要である。

### 2. これまでの経緯

お茶の水女子大学は、法人化された平成16年度以降、情報に関連して、次のような規則等を定めてきた。なお、国立大学法人を(国)と略記している。

- ① 平成16年4月 (国)お茶の水女子大学ウェブ・ページ運用指針
- ② 平成16年4月 (国)お茶の水女子大学ウェブ・ページ運用マニュアル
- ③ 平成16年4月 (国)お茶の水女子大学ウェブ・ページ運営規則
- ④ 平成16年7月 (国)お茶の水女子大学情報セキュリティポリシー
- ⑤ 平成17年3月 (国)お茶の水女子大学個人情報の管理に関する規則
- ⑥ 平成17年3月 (国)お茶の水女子大学個人情報公開取扱要項

⑦ 平成17年3月 (国)お茶の水女子大学個人情報の開示・訂正・利用停止審査基準

これらの規則等に基づき、附属幼、小、中、高の教員と管理職を委員とする情報専門委員会を中心に、平成16年度に情報セキュリティ指針を、平成17年度は個人情報の管理、ウェブ・ページの管理・運用について、共通の方針や基準を定めた。今年度は教職員向けの情報取扱マニュアルを、児童・生徒向けのマニュアル、管理マニュアルを作成しつつある。

### 3. 解決に向けて

個人情報の収集・保管・更新・破棄などの方法については、附属校園が協同して基準を定め、運用し、ウェブページ等のチェック機能を果たすための管理組織を作成することが必要になっている。

#### (1) 組織

附属学校部及び各附属校園の情報管理組織は、規則⑤に基づいて次のように構成される。情報専門委員は、アクセス制御、バックアップ、端末の限定など、附属校園の個人情報の管理を補助する。

- ・総括保護管理者（情報担当の副学長）
- ・保護管理者（附属学校部長及び各校園長）：保有個人情報を適切に管理する。
- ・保護担当者（各校園の副校長）：保護管理者を補佐し、保有個人情報の管理に関する事務を行う。
- ・情報専門委員：保有個人情報のシステム設計など情報管理に関する事務を行う。

保護管理者は、保有個人情報の秘匿性等その内容に応じて情報にアクセスする権限を有する者を指定する。実際は、各校園のコンピュータ委員がこれに当たる。

#### (2) 管理業務

附属校園の担当者は、将来的に次のような情報管理((a)～(e))、IT管理((f)、(g))、安全管理((h)～(j))などの業務を保護管理者の責任のもとで行う必要があると考えられる。

- (a) **情報・媒体の管理**：個人情報の収集、保有個人情報の複製、送信、記録媒体の外部への送信または持出しの場合の措置、保有個人情報の内容に誤りを発見した場合の措置等を定める。
- (b) **台帳の整備**：保護管理者は保有個人情報の内容に応じて台帳等を整備し、利用及び保管等について記録する。
- (c) **廃棄**：保有個人情報またはその媒体が不要になった場合の措置を定める。
- (d) **情報ファイルの整備**：情報開示請求等に備えて、保有個人情報ファイル簿（現在は、学籍、授業料、入学試験、卒業者、履修・成績、健康診断、図書館利用者）を整備し、記載事項に変更があった場合、新たに保有した場合及び保有をやめた場合は総括保護管理者に提出する。
- (e) **外部委託**：保有個人情報に係わる業務を外部に委託する場合、秘密保持、再委託の制限、複製の制限、漏洩等の事案発生時の対応、委託終了時における消去及び媒体返却、違反した場合の契

約解除などの事項を作成する。

- (f) **パスワードとアクセス**：必要に応じてパスワードを用いて権限を識別し、その管理について定め、アクセス状況を記録し、定期的に分析する。また、アクセス記録の改ざんや不正な消去防止のための措置をとる。また、保有個人情報の秘匿等その内容に応じて、アクセスする権限を有する者だけがアクセスできる保有個人情報を定める。
- (g) **端末及びサーバの管理**：端末の盗難又は紛失の防止措置、第三者に閲覧されないための措置を定める。また、基幹的なサーバ等の機器を設置する部屋の施錠と入退室の記録などの管理を行い、災害時に備え、情報サーバ室に耐震、防火等の設備を施す。
- (h) **システム設計**：保有個人情報に係わる情報システムの設計を行う。
- (i) **研修**：附属校園の教員に対して実施する保有個人情報の取扱いの教育研修へ参加する機会を与える。また、生徒に対して、個人情報に関する教育を行う。
- (j) **安全対策**：保有個人情報の漏洩等、安全確保の上で問題となる事案が発生した場合の対処方法を作成する。
- (k) **例外措置**：保有個人情報を第三者に提供する例外項目を作成する。例えば、本人の同意がある場合、本人または第三者の生命・身体・財産・権利に緊急の危険があり、本人通知が困難あるいは不可能な場合、法令に基づく場合など。